
	<b>D4.2.2 Prototype Mountain Rescue Service Trial</b>	
---	---	---



**Project no. 035003**

**u-2010**

## **Ubiquitous IP-centric Government & Enterprise Next Generation Networks Vision 2010**

Instrument: Integrated Project

Thematic Priority 2

### **D4.2.2 Prototype Mountain Rescue Service Trial**

Due date of deliverable: 31<sup>st</sup> July 2009

Submission date: 16<sup>th</sup> September 2009

Start date of project: May 1<sup>st</sup> 2006

Duration: 36 months

Organisation name of lead contractor for this deliverable: Lancaster University

Revision: v1.0

<b>Project co-funded by the European Commission within the Sixth Framework Programme (2002-2006)</b>		
<b>Dissemination Level</b>		
<b>PU</b>	Public	✓
<b>PP</b>	Restricted to other programme participants (including the Commission Services)	
<b>RE</b>	Restricted to a group specified by the consortium (including the Commission Services)	
<b>CO</b>	Confidential, only for members of the consortium (including the Commission Services)	

	<p align="center"><b>D4.2.2 Prototype Mountain Rescue Service Trial</b></p>	
---	---	---

## **Abstract**

The purpose of this document is to outline the prototype implementation for the Mountain Rescue service trial. It provides an overall picture of which components have been implemented, how they work together and the methodology of the trial. It is the conclusion of 18 months of discussions, analyses, development and lab/field trials.

All the results from the Mountain Rescue trial are reported and analysed in the companion deliverable, D4.2.3 Report on the Mountain Rescue Service Trial.

### **Keywords:**

Mountain Rescue, Mobile Networks, MANEMO, Presence Management, Video streams, Voice Service, VoIP, Directory Services.

## History of Change

Issue	Status	Date	Details	Responsible
v0.1	Draft	18/11/08	General document skeleton and ToC.	Martin Dunmore
v0.2	Draft	20/11/08	Added chapters for Introduction and What Has Been Implemented	Martin Dunmore
v0.3	Draft	15/12/08	Minor corrections	Martin Dunmore
V0.4	Draft	27/05/09	Update on backpack routers.	Martin Dunmore
V0.5	Draft	17/06/09	Update after Slovenia demo.	Martin Dunmore
V0.6	Draft	03/07/09	Comprehensive restructuring	Martin Dunmore
v0.7	Draft	24/07/09	Added chapter on u-2010 architecture.	Martin Dunmore
v0.8	Draft	23/08/09	Added text for handover management of MANEMO routers	Ben McCarthy, Martin Dunmore
v0.9	Draft	09/09/08	Added Voice Service. Final draft for internal review	Martin Dunmore
v1.0	Final	14/09/09	Minor changes in response to reviewers' comments	Martin Dunmore

## Table of Contents

<b>EXECUTIVE SUMMARY .....</b>	<b>8</b>
<b>1. INTRODUCTION .....</b>	<b>9</b>
<b>2. THE MOUNTAIN RESCUE SERVICE SCENARIO .....</b>	<b>10</b>
2.1. SCENARIO DESCRIPTION .....	10
2.2. DEFINITION OF USERS AND ROLES.....	12
<b>3. IMPLEMENTATION ACCORDING TO THE U-2010 ARCHITECTURE .....</b>	<b>15</b>
3.1. MOBILE UNITS.....	16
3.2. STATIC ENTITIES.....	17
3.3. INCIDENT AREA NETWORK.....	17
3.4. MOBILE COMMAND POST .....	18
3.5. WIDE AREA NETWORK .....	19
3.6. CRISIS CENTRE .....	19
<b>4. PROTOTYPE DESCRIPTION / WHAT HAS BEEN IMPLEMENTED.....</b>	<b>21</b>
4.1. SATELLITE AND BACKHAUL LINKS .....	22
4.2. BACKPACK ROUTERS.....	29
4.3. MANEMO .....	31
4.3.1. Intelligent Handover Management.....	33
4.4. PRESENCE MANAGEMENT AND MESSAGING SERVICES.....	35
4.5. ALARM SERVICE.....	38
4.6. DIRECTORY SERVICE .....	39
4.7. VOICE SERVICE.....	41
4.8. VIDEO AND PICTURE SERVICES.....	43
4.9. SEARCH THEORY .....	46
4.10. WHAT WILL NOT BE IMPLEMENTED .....	48
4.10.1. Sensor Service .....	48
4.10.2. Directory Service.....	49
4.10.3. Integrated Voice Service .....	49
<b>5. TRIAL METHODOLOGY .....</b>	<b>50</b>
5.1. PRESENCE MANAGEMENT SERVICE TESTS.....	50
5.2. BACKPACK ROUTER TESTS.....	51
5.3. SATELLITE AND BACKHAUL LINK TESTS .....	52
5.4. COMMAND AND CONTROL SOFTWARE TESTS .....	53
5.5. VOICE SERVICE TESTS .....	53
5.5.1. Test Procedures .....	54
5.5.2. Test Scenarios .....	54
5.6. VIDEO SERVICES TESTS .....	56
5.7. MANEMO TESTS.....	57
5.8. MANEMO AND VOICE SERVICE .....	57
5.9. MANEMO AND VIDEO SERVICE .....	59
<b>REFERENCES.....</b>	<b>61</b>
<b>ACRONYMS.....</b>	<b>62</b>

## List of Figures

Figure 1 Rescue Network Hierarchy .....	10
Figure 2 General Scenario Concept.....	11
Figure 3 CMRT Search Region.....	14
Figure 4 u-2010 System .....	15
Figure 5 NSV-4 Mobile Units .....	16
Figure 6 NSV-4 Incident Area Network (IAN).....	17
Figure 7 NSV-4 Mobile Command Post .....	18
Figure 8 NSV-4 Crisis Centre .....	20
Figure 9 Software Overview .....	21
Figure 10 The CLEO Network.....	22
Figure 11 Intended PoP Locations .....	23
Figure 12 Envisaged Network Deployment (Longterm).....	24
Figure 13 Testing Locations within the CMRT Search Region .....	26
Figure 14 5 GHz Radio Relay on Low Fell.....	27
Figure 15 5 GHz Radio Link at Rannerdale.....	27
Figure 16 Astra2Connect Link with Grasmoor in Background .....	28
Figure 17 “Communications Vehicle” .....	29
Figure 18 Inside the Backpack Router .....	30
Figure 19 Backpack and Router      Figure 20 Backpack Router worn by Rescuer.....	31
Figure 21 UMA Prototype Development Testbed.....	32
Figure 22 Connectivity Option Example.....	34
Figure 23 Access Point Information.....	35
Figure 24 Main Tab of Client Application.....	36
Figure 25 Screenshot of the PMS Server Application.....	38
Figure 26 Screenshot of the Mountain Rescue Alarm Service using AlarmTilt.....	39
Figure 27 Simple Large Button GUI for Voice Service Client .....	42
Figure 28 Panasonic BL-C121 Network Camera [16] .....	44
Figure 29 Screenshot of the Video Web Service (Panasonic BL-C121).....	45
Figure 30 Probability distribution .....	47
Figure 31 Assigning a Search Team.....	48
Figure 32 Voice Service - Local Initial Testing .....	55
Figure 33 Voice Service – Local Base Tests.....	55
Figure 34 Voice Service - Internet Tests.....	56



	<p align="center"><b>D4.2.2 Prototype Mountain Rescue Service Trial</b></p>	
---	---	---

Figure 35 Voice Service and MANEMO .....	58
Figure 36 Voice Service and MANEMO – Long distance.....	58
Figure 37 Voice Service - Large Number of Wireless Hops.....	59

## List of Tables

Table 1 Users and Roles.....	12
Table 2 - Members Table Schema.....	40
Table 3 - Devices Table Schema.....	40
Table 4 - Incidents Table Schema .....	41
Table 5 - Incident_Rescuers Table Schema .....	41

## Executive Summary

Deliverable 4.2.2 ‘Prototype Mountain Rescue Service Trial’ presents an overview of the various service components that form the prototype implementation of the Mountain Rescue Service trial. This document provides an overall picture of which components have been implemented, how they work together and the methodology of the trial.

The application scenario that is described in this document is based on the Mountain Rescue service scenario (as described in the u-2010 deliverables D1.1.1 Reference scenarios based on user studies [1], D1.1.2 Functional requirements for networks and services [2] and D4.2.1 Report on the Mountain Rescue Service Concept [8]). The scenario has been further enhanced based on ongoing discussions with the CMRT (Cockermouth Mountain Rescue Team) and experiences with development and deployment testing. Some of the components, notably the PMS (presence management service) and backpack routers, have been demonstrated in the Slovenian Mountain Rescue Service scenario. The implementation of this scenario is described in deliverable D4.5.2 Report on Mountain Rescue Service Implemented in Slovenia [10].

The implementation of the Mountain Rescue Service trial is based around two areas: the communications infrastructure and the CaC (command and control) software located at the rescue team’s headquarters. The communications infrastructure comprises ‘rapid-response’ PoPs, which connect the IAN (Incident Area Network) to the global Internet. The IAN, which is the communications network that serves the geographical area around the emergency incident, is served by miniaturised, lightweight backpack routers running the MANEMO protocol suite. These backpack routers allow the IAN to be dynamically extended and follows the movement of the rescue workers. Since any search and rescue mission involves relatively frequent and unpredictable movement of the rescue workers, it is essential for the IAN to be able to adapt in this manner. The CaC software provides a portal for the mission controller at headquarters to use, monitor and manage the various services available. These services include the PMS, an alarm service, a voice service based on a bespoke VoIP system, and a combined video and picture service.

Most of the component tests described in the Trial Methodology chapter have been completed including those for the PMS (presence management service), backpack routers, CaC (command and control) software, satellite/backhaul links, voice service, video service and MANEMO protocol suite. Some tests are still ongoing, mostly related to voice and video service testing in conjunction with MANEMO, and these will be completed through September. In any case, all results from the Mountain Rescue trial are reported and analysed in the companion deliverable, D4.2.3 Report on the Mountain Rescue Service Trial [9].



	<p align="center"><b>D4.2.2 Prototype Mountain Rescue Service Trial</b></p>	
---	---	---

## 1. Introduction

Deliverable 4.2.2 ‘Prototype Mountain Rescue Service Trial’ presents an overview of the various service components that form the prototype implementation of the Mountain Rescue Service trial. Since some of the design and development details of these components are described in more detail in other deliverables, they are not described in detail here. Rather, this document provides an overall picture of which components have been implemented, how they work together and the methodology of the trial.

However, this document does not present detailed results from the trial tests, nor analysis, conclusions and recommendations based on those results. All of this information is provided in the companion deliverable D4.2.3 Report on the Mountain Rescue Service Trial [9].

The application scenario described in this document is based on the Mountain Rescue service scenario, which is described in the u-2010 deliverables D1.1.1 Reference scenarios based on user studies [1], D1.1.2 Functional requirements for networks and services [2] and D4.2.1 Report on the Mountain Rescue Service Concept [8]. The scenario has been further enhanced based on ongoing discussions with the CMRT (Cockermouth Mountain Rescue Team) and experiences with development and early deployment testing. The CMRT is one of 12 rescue teams in the English Lake District and covers a search area of around 600Km<sup>2</sup>. It operates 365 days a year with rescue workers totalling 1500 hours per year on rescues. Despite this commitment, the CMRT is a registered charity and is funded solely by voluntary contributions; the rescue workers themselves are all unpaid volunteers [11].

The rest of this document is structured as follows: the following chapter briefly describes the general Mountain Rescue service scenario and defines the users and their roles. Chapter Three illustrates which components of the general u-2010 architecture are implemented in the Mountain Rescue service solution. Chapter Four provides an overview of all the service components that have been implemented to realise the prototype Mountain Rescue service trial and details the service components that, although desirable, will not be implemented within the lifetime of u-2010. Chapter Five discusses the trial methodology, what the objectives of the trial are and how the trial is broken down into various testing scenarios.

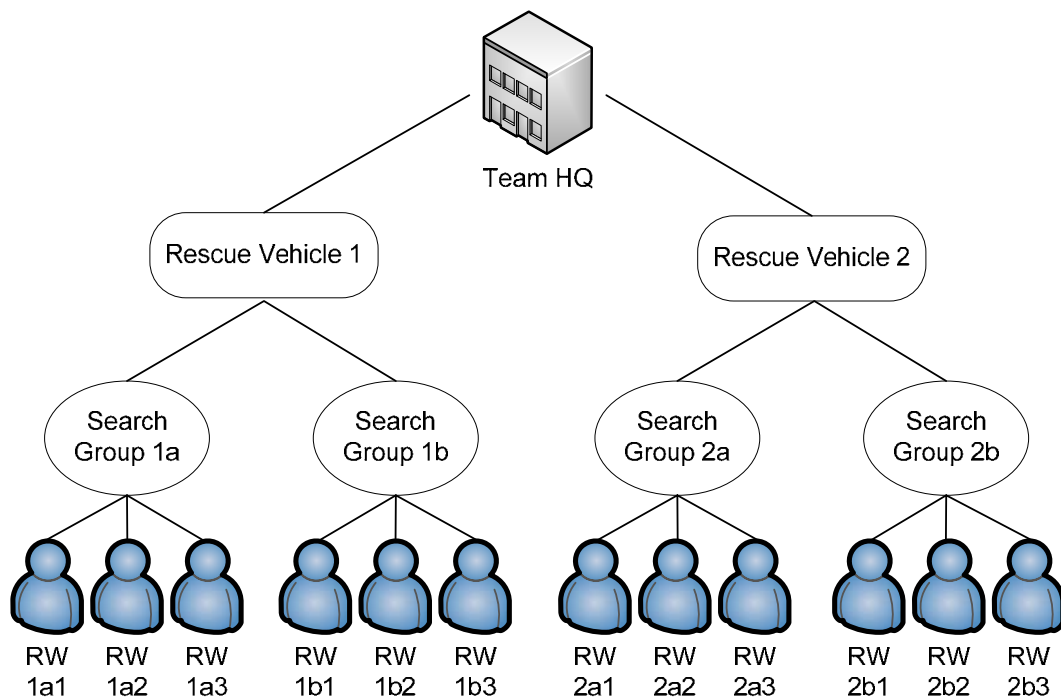
## 2. The Mountain Rescue Service Scenario

Lancaster University lies on the border of the English Lake District (located in the county of Cumbria), which is extremely popular for a wide variety of recreational activities including hiking, climbing, fell running, canoeing, sailing and camping. Recreation and tourism attributed to the English Lake District provides the primary source of income for the area. The various Mountain Rescue teams of Cumbria are often first responders for a wide variety of incidents (in addition to their usual mountain-related incidents) and provide close support to the traditional first responders such as ambulance, fire and police services. For example, many Mountain Rescue Team volunteers attended the Grayrigg train accident in 2007 to provide assistance to the walking wounded and unhurt survivors [19].

In cooperation with the CMRT (Cockermouth Mountain Rescue Team), Lancaster University is deploying backpack IPv6 mobile routers to provide the team with an on-mountain data networking solution. Lancaster University is also responsible for the network connectivity of all the schools and colleges in the Lancaster and Cumbria counties via the CLEO (Cumbria and Lancashire Education Online - <http://www.cleo.net.uk>) initiative, which uses CANLMAN (Cumbria And North Lancashire Metropolitan Area Network – <http://www.canlman.net.uk>). The importance of this is that the University can provide the backhaul network access that the Mountain Rescue service's mobile networks can rely on.

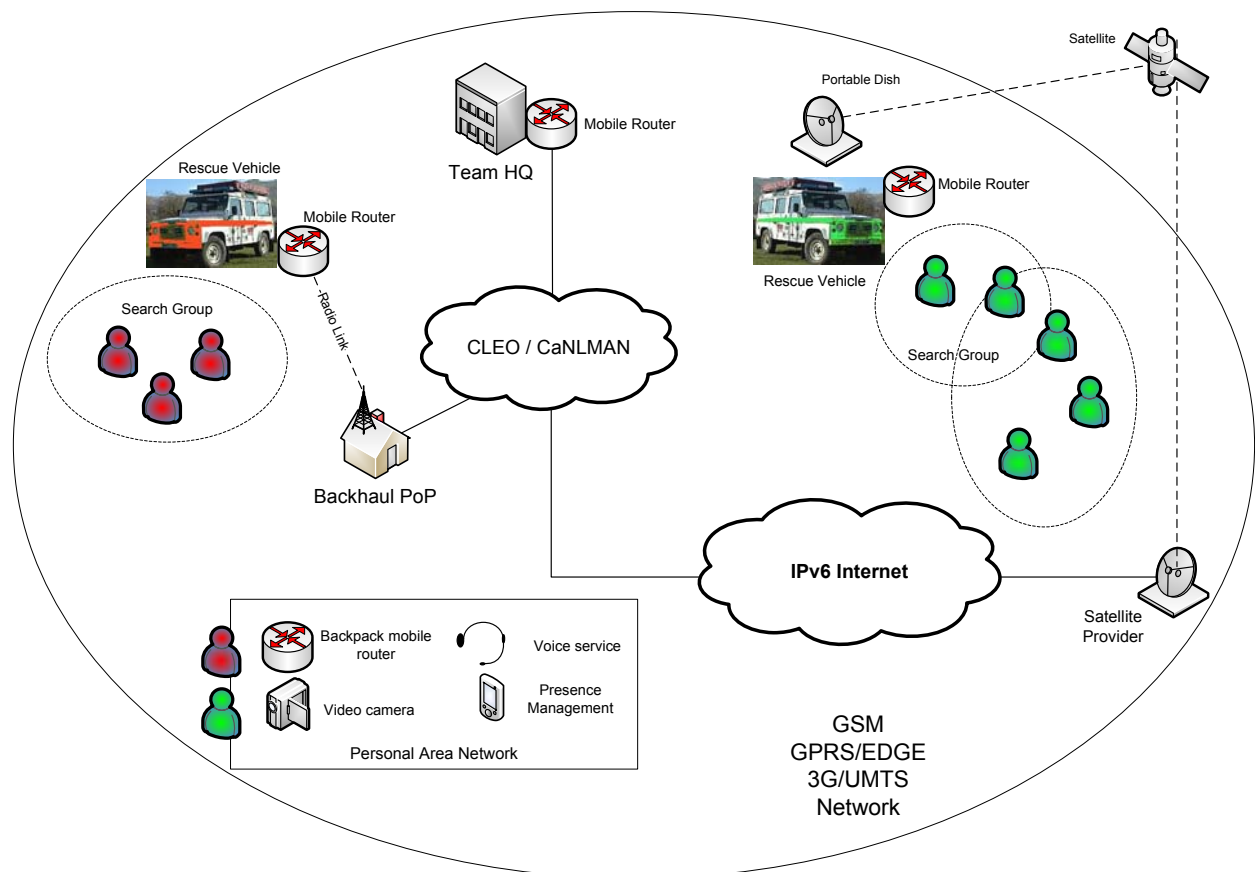
### 2.1. Scenario Description

In a typical Mountain Rescue operation, each Mountain Rescue Team (e.g. CMRT) will have several individual rescue workers, each assigned to a search group, which is further linked to a base vehicle. This leads to an obvious hierarchical relationship as depicted in Figure 1.



**Figure 1 Rescue Network Hierarchy**

However, these relationships are somewhat relaxed in that rescue vehicles, search groups, and individual rescue workers may sometimes change their ‘points of attachment’ as a search operation evolves. From a networking perspective, each search group represents one distinct local network, with its rescue workers being nodes on that network. Since each search group can change location, the search group network becomes mobile. In a similar fashion, the rescue vehicles are their own distinct mobile networks, with only the Team HQ remaining static. To further complicate matters, any rescue worker may move in such a fashion that they attach to a network of a different search group, or even a different rescue vehicle. Fortunately, the organisation of such a complex conglomeration of mobile nodes and networks can be solved using IPv6 and MANEMO (MANET and NEMO) protocols. This is discussed in detail in deliverable D2.2.2 Report on u-2010 Mobility Solution [4]. However, this report (D4.2.2) is more concerned with where the IPv6 and MANEMO solution fits into the general Mountain Rescue scenario and how it is used, rather than the internal details of the solution.



**Figure 2 General Scenario Concept**

Enabling efficient communication for the Mountain Rescue scenario can be achieved by interconnecting the remote search areas with the HQ of the team. However, providing sufficient network connectivity in such remote rural locations is very challenging. The choice of network infrastructure is limited as wired connectivity is restricted to major towns. In addition, fixed public networks such as GSM, GPRS and UMTS have patchy or non-existent coverage in some areas. Nevertheless, any connectivity provided by CANLMAN, plus any public wireless networks, plus possible satellite connectivity (provided by u-2010), can all be exploited by IPv6 mobile routers running MANEMO. Furthermore, we can build coverage ‘on-demand’ by co-locating portable 802.11/Wi-Fi or 802.16/WiMAX access points or base stations with the

mobile routers. Figure 2 illustrates a general overview of the deployment concept for the Mountain Rescue scenario.

Mobile routers are located with the rescue vehicles. Using high gain directional antennae, we can project a hotspot of connectivity over the area being covered by the search groups assigned to that vehicle. Network technologies such as 802.11 and/or 802.16 can be used to achieve this connectivity. The vehicle mobile routers can also use GPRS/UMTS connectivity as the uplink to the Team HQ. Other options are to support point-to-point or point-to-multipoint radio links (e.g. Wi-Fi or WiMAX) or bi-directional satellite links via appropriate antenna and transceiver assemblies on the rescue vehicles connected to the mobile routers. Small form factor mobile routers are integrated into the backpacks of designated rescue workers thus providing connectivity for each search group. In general, each search group will have its own 802.11 hotspot to which rescue workers can connect. In this way, rescue workers are not only connected to others in the same search group, but also with the Team HQ (located many kilometres away) via their rescue vehicle and also with rescue workers from other search groups via the wireless networks of different search groups and the search vehicles. Any rescue worker with connectivity to any search group's wireless network has connectivity to the overall network. Since the mobile routers can also bridge different wireless networks, the effective coverage area can be expanded. Yet, it is IPv6 and MANEMO that truly facilitates this capability. Using IPv6 neighbour discovery a rescue worker's device will automatically detect the network of a different search group and attach to it without any user involvement (assuming the usual network is not available). Any existing applications would normally be broken at this point. However, using MANEMO, the applications can carry on using the same IPv6 addresses and do not even realise that their device's attachment point has changed.

## 2.2. Definition of Users and Roles

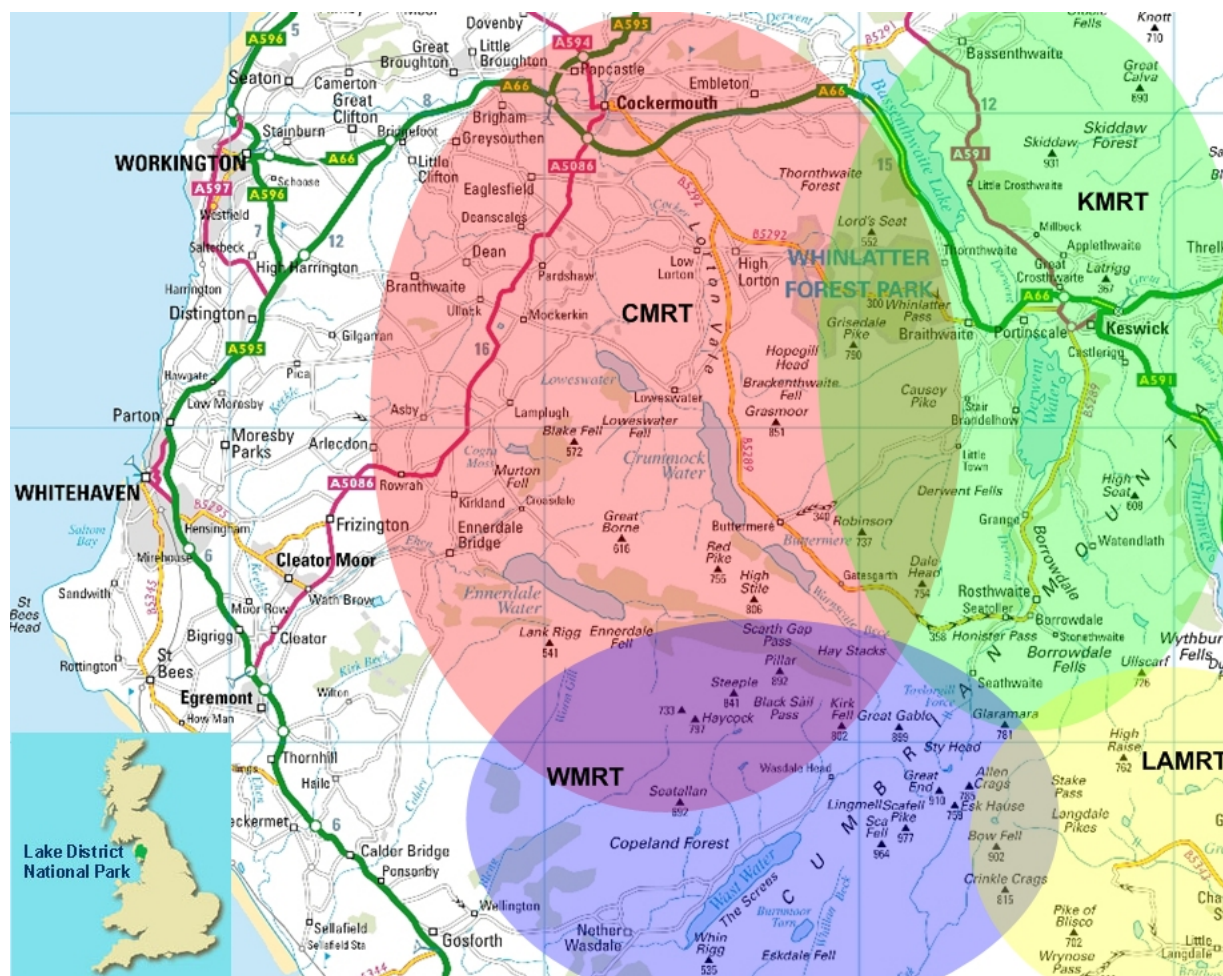
The following table defines the user roles that were identified in the Mountain Rescue Scenario

**Table 1 Users and Roles**

User	Role
Team HQ	The headquarters of the Mountain Rescue team. This is where all search and rescue operations are controlled, managed and monitored. Typically, the HQ will be located many kilometres from the search areas
Controller	The controller is located in the Team HQ and is responsible for organising the overall search and rescue operation from the initial emergency call until the mission is terminated.
Police	The Police will receive the initial emergency call and are responsible for contacting the controller at the Team HQ and passing on all the details of the incident. The Police may also take part in the search and rescue operation by, for example, searching car parks for the missing person's vehicle or calling hotels and campsites to see if they have any information on the missing person.

User	Role
Informant	The informant is the person who makes the emergency call requesting Mountain Rescue service. This may be the casualty themselves or a third party. Depending on the situation, the information provided by the informant can range from specific to extremely vague. The informant will be in voice contact with the controller after the Police have contacted the HQ.
Group Leaders	Group Leaders are assigned to each search group and have the responsibility of making sure the search group follows the intended search patterns.
Rescue Workers	Rescue workers are the unpaid volunteers that make up the Mountain Rescue team. They are responsible for conducting the search and rescue operation according to the intended plan. Group Leaders are also Rescue Workers.
Ambulance Paramedics	Ambulance Paramedics attend to the scene when they are signalled to do so by the controller at HQ. Since it can take several hours to locate a missing person, there is little sense in the ambulance departing for an unknown destination when the emergency call is first made. Ambulance paramedics wait by the nearest roadside location (identified by the controller) for the Rescue Workers to carry the casualty down the mountain.
Hospital	The hospital is responsible for the long-term treatment of the casualty. The emergency room of the hospital is placed on standby and informed of the casualty's condition as the search and rescue operation progresses.
Air Force	If the casualty is in an inaccessible position, or if his injuries are life threatening, the controller will request an airlift to hospital. The air force is placed on standby when the casualty is located and then stood down or scrambled once the team doctor and group leader(s) have determined the right course of action.





### Figure 3 CMRT Search Region

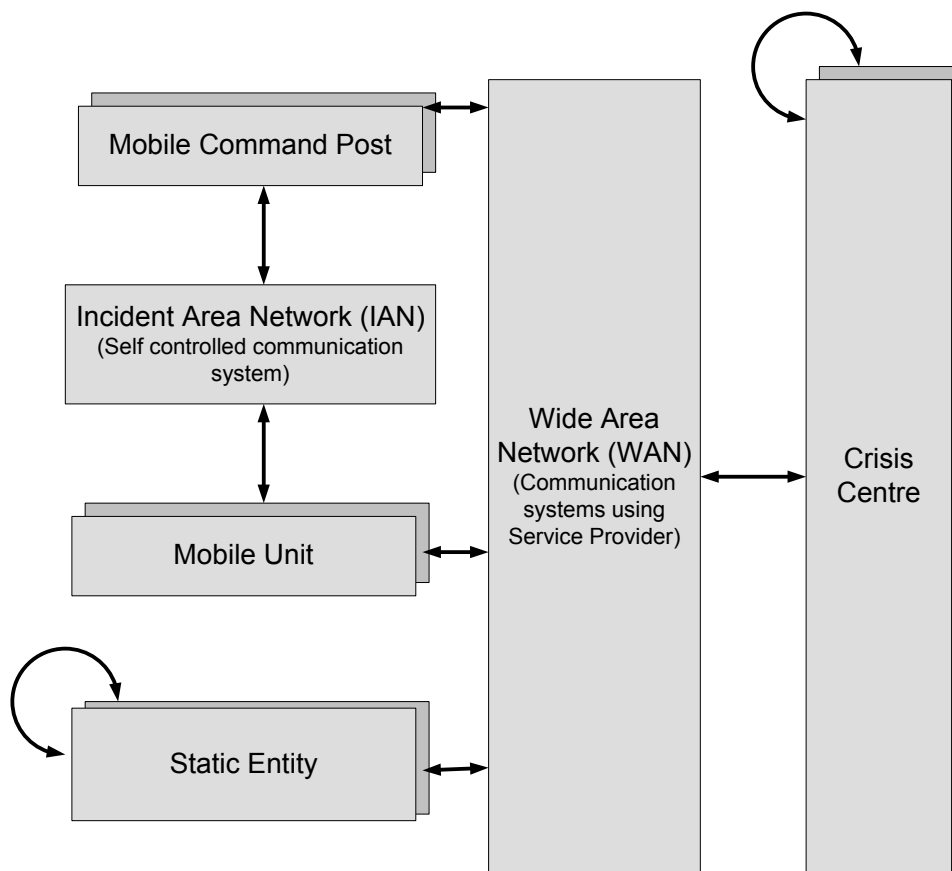
In order to avoid repeating too much information here, please refer to deliverable D4.2.1 Report on the Mountain Rescue Service Concept [8] for a more detailed description of the Mountain Rescue scenario.

Figure 3 highlights the main search area of the Cocker-mouth Mountain Rescue Team (CMRT). From the figure, it is clear that there are times when the CMRT will need to cooperate with other mountain rescue teams on a search and rescue operation. It is also clear that the CMRT is responsible for a large search area, indeed larger than can be accurately highlighted on the map. This map only shows the most likely area for a search and rescue operation, although the CMRT may be called to assist the coastguard during a sea rescue as well as other mountain rescue teams that do not appear on the map. Suffice to say, the Mountain Rescue prototype must serve the primary search region of the CMRT and preferably all the secondary areas too.

### 3. Implementation According to the u-2010 Architecture

This chapter describes which elements of the defined u-2010 architecture are implemented in the Mountain Rescue service trial. All of the architecture elements described in this chapter are presented in detail in D2.1.2 u-2010 Architecture [3].

Figure 4 shows a high-level view of the u-2010 system architecture. This global view of the architecture is composed of different subsystems, which interact and communicate between themselves.



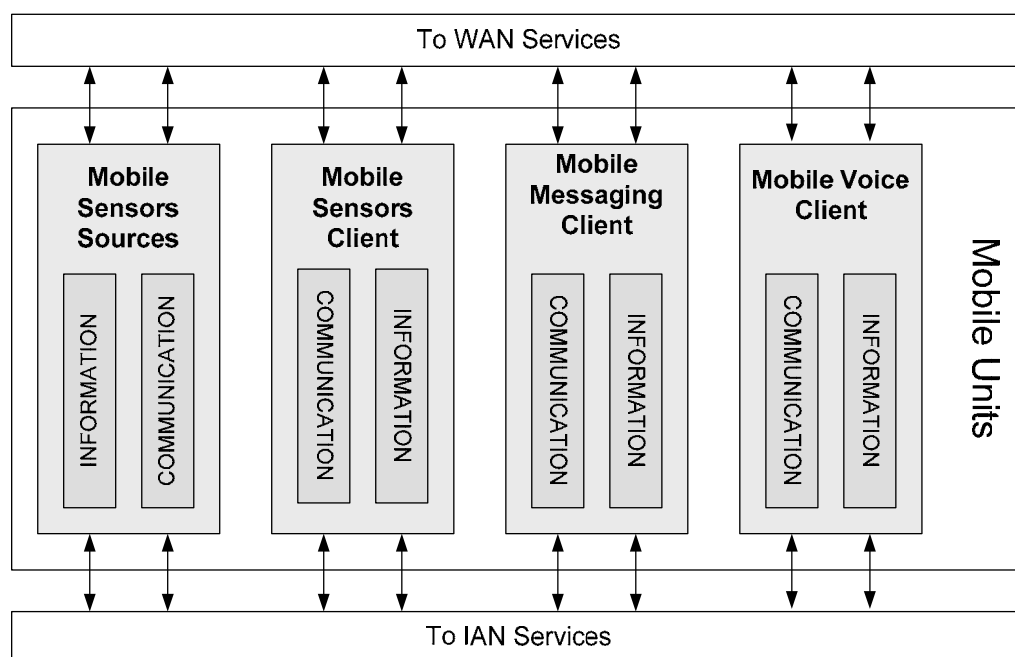
**Figure 4 u-2010 System**

The instantiation of a specific scenario or a particular emergency within a scenario, need not contain all these subsystems, and may even contain others. However, this set of subsystems gives a typical instantiation for most emergency scenarios. We will now describe each subsystem with respect to its applicability in the Mountain Rescue scenario.

### 3.1. Mobile Units

The Mobile Units subsystem represents the mobile end-devices, which are used in public safety scenarios by the mobile teams sent to an emergency. Their key functionality is to realise a mobile user's access via a Human to Computer Interface (HCI) Device for information delivery. To permit mobility, the Mobile Units may have immediate WAN access (e.g. UMTS). Alternatively, the Mobile Units may communicate and share information with each other or with a Mobile Command Post via the Incident Area Network (IAN).

In the Mountain Rescue scenario, the Mobile Units are the end devices carried by rescue workers and group leaders (see Table 1) conducting the search and rescue operation.



**Figure 5 NSV-4 Mobile Units**

The internal architecture of the Mobile Units is shown in Figure 5. The rescue workers and group leaders carry mobile devices (in the Mountain Rescue service trial, we use PDAs) that contain clients for voice and message services. Location information for the Presence Management Service (see section 4.4) is included in the messaging client. The voice service is described in section 4.7. Normally, the PDAs communicate via the IAN but have the capability to communicate via the WAN if this is more appropriate than the IAN, or the IAN is unavailable. The sensor service is not implemented in the Mountain Rescue service trial although we have implemented sensor gateway capability on the backpack routers. These backpack routers (see section 4.2) are carried by the rescue workers and group leaders (though not necessarily by all) and so can also be considered as Mobile Units with respect to the defined u-2010 architecture.



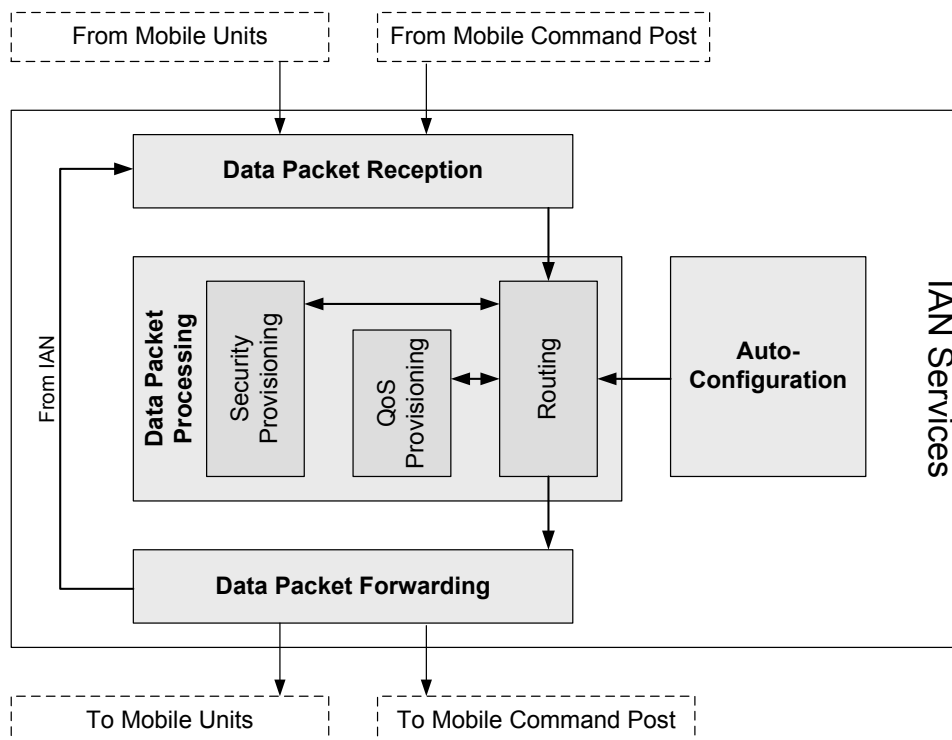
### 3.2. Static Entities

The Static Entities represent the permanent, fixed facilities of an agency. Actually, these fixed entities represent all the different functional entities such as logistic, monitoring or permanent representation and liaison teams. The Static Entities are similar to Mobile Units, with the communication functionalities being the same. The only change comes from the fact that the Static Entities do not require the use of the IAN.

In the Mountain Rescue scenario in the UK, there are no *applicable* Static Entities. Only minor entities such as stretcher boxes and mountain shelters exist, but these are not applicable to the u-2010 architecture. However, more applicable Static Entities (e.g. fixed emergency voice/data points) could conceivably exist in other EU countries and/or in the future. In any case, we have not implemented any Static Entities in the Mountain Rescue service trial.

### 3.3. Incident Area Network

The Incident Area Network (IAN) subsystem is intended to be a flexible and rapidly deployable communication network, which covers the area around an incident. It provides communication to the entities present in the incident area, typically to Mobile Units and Mobile Command Posts, and potentially also to Static sub-entities in the incident area. The IAN needs to be quickly and easily deployable and should not depend on any pre-installed infrastructure, as this may be destroyed or unavailable during an incident. The u-2010 project mainly investigates the usage of mobile ad-hoc networks to form the IAN, since they can provide a rapid-response, flexible and secure IP-based communications solution. Alternatively, digital terrestrial radio systems used in direct mode could be considered for the IAN. Mobile Units attached to the IAN can be provided with access to WAN (and therefore remote entities) via the Mobile Command Post.

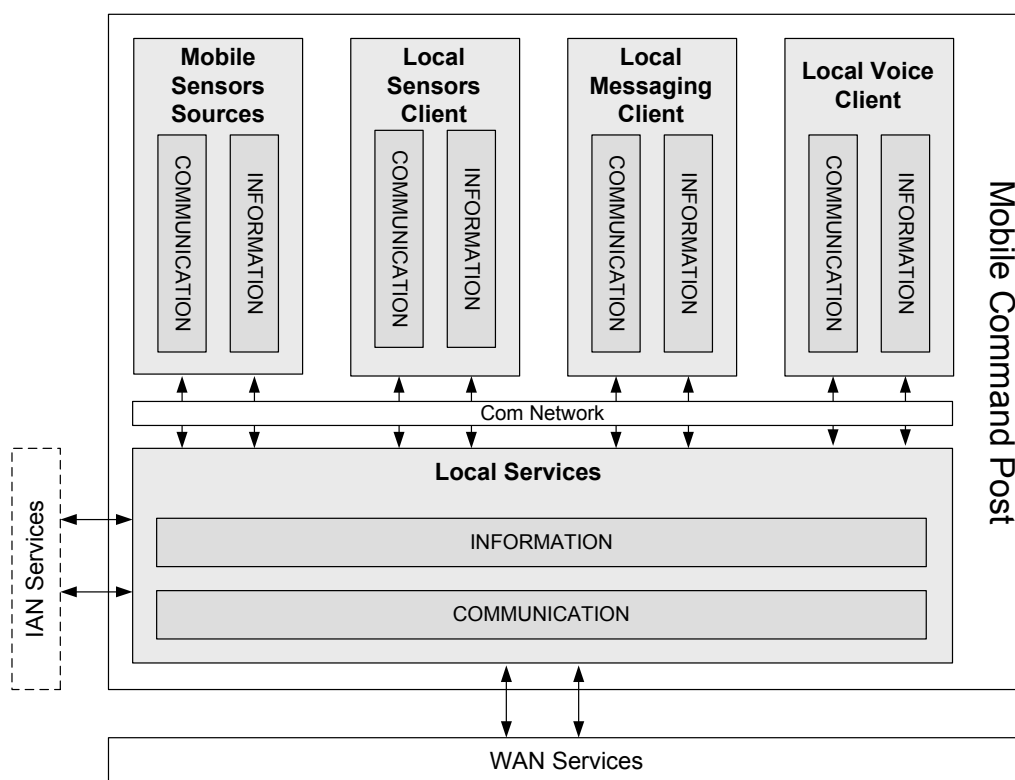


**Figure 6 NSV-4 Incident Area Network (IAN)**

The IAN in the Mountain Rescue service trial is provided by equipment from the rescue vehicles at the Mobile Command Posts. The IAN supplies connectivity in the vicinity of the rescue vehicles and is further extended into the areas that are being searched. Perhaps the most important part of the IAN are the backpack routers. The backpack routers, which are portable, small form factor, battery-operated, multi-interfaced routers that run the MANEMO protocol suite. It is the combination of these backpack routers and MANEMO that extends the IAN into the search areas as the rescue workers roam away from the Mobile Command Post. Moreover, the backpack routers have the ability to bypass the Mobile Command Post when routing to the WAN. In other words, traffic can be sent to the WAN directly from the backpack routers should the WAN connection at the Mobile Command Post be inappropriate or unavailable. The backpack routers are presented in section 4.2 and MANEMO is presented in section 4.3.

### 3.4. Mobile Command Post

The Mobile Command Post subsystem is a mobile and easily deployable Command Post that plays the role of a local Crisis Centre in the vicinity of the incident. The Mobile Command Post may host or replicate services that are normally provided at the Crisis Centre. An example of this is the provision of monitoring services, video servers and directory services at the Mobile Command Post. The Mobile Command Post may also provide a relaying or caching role for these services. The other subsystems of the u-2010 system architecture can be connected to the Mobile Command Post via the IAN or the WAN depending on the nature and location of the subsystem.



**Figure 7 NSV-4 Mobile Command Post**

	<p align="center"><b>D4.2.2 Prototype Mountain Rescue Service Trial</b></p>	
---	---	---

In the Mountain Rescue service trial, the Mobile Command Post is generally represented by one or more rescue vehicles, which establish a location from which the search groups operate. In some incidents, there may be multiple Mobile Command Posts due to there being a large search area to cover. Mobile Command Posts will usually connect to each other via the WAN. However, it is conceivably possible that they can connect via the IAN attached to one or both Mobile Command Posts. This can occur if the backpack routers of different IANs come into range of each other, or if one IAN comes into the range of another Mobile Command Post.

### **3.5. Wide Area Network**

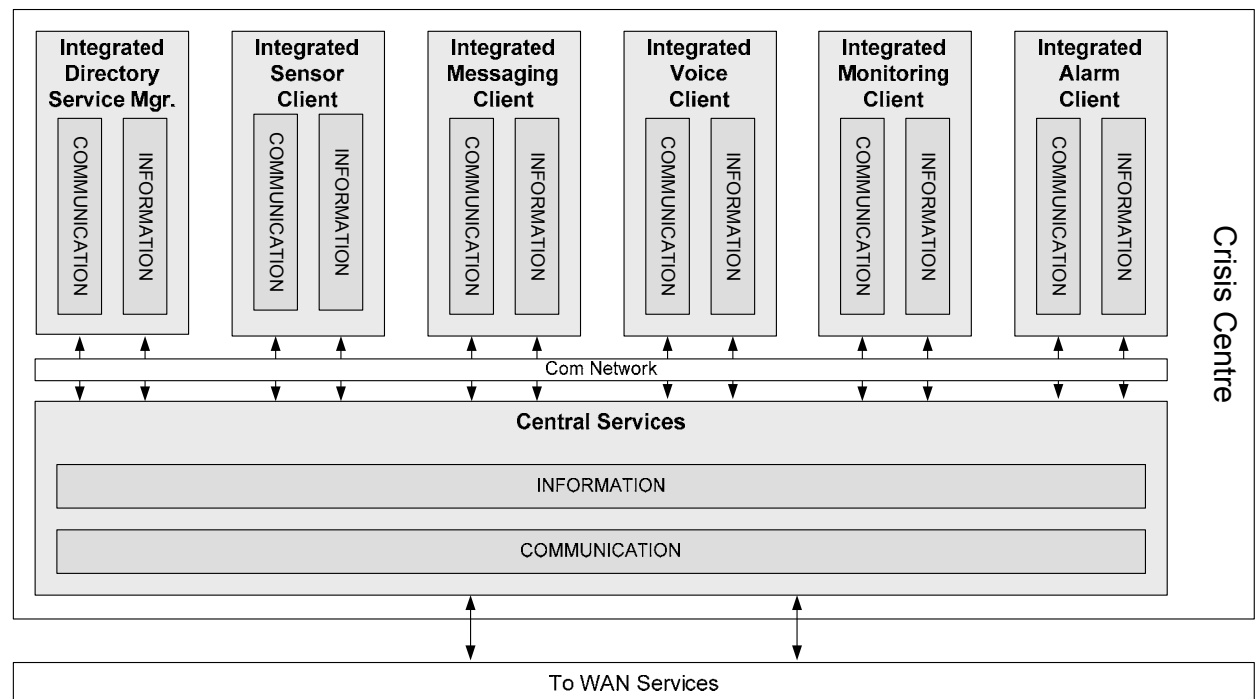
This part of the u-2010 architecture represents the available network technologies that give global Internet access that can be accessed by the different units/entities. In u-2010, we assume that the networks operate over the IP and particularly IPv6. Thus, all of the services in the Mountain Rescue service trial operate over IPv6. Thus any WAN connections providing IPv4-only access necessitate the use of IPv6 transition mechanisms such as tunnelling. A good example of this in the Mountain Rescue service is the use of IPv6-in-IPv4 tunnelling over the satellite WAN link from the Mobile Command Post (rescue vehicle) to the Crisis Centre (Team Headquarters).

### **3.6. Crisis Centre**

The Crisis Centre subsystem is composed of the main (e.g. regional or national) crises centre and a given number of operational headquarters. It represents the physical and logical fixed infrastructures always activated in preparation for crisis management.

A given facility can be used either as a national crisis centre or as an operational headquarters. The reason can be explained as an escalation procedure. Indeed, for all emergencies, an appropriate operational headquarters is required. This allows a reporting and communication link to be maintained with the Mobile Units. Depending on the scale of the emergency, the Crisis Centre may delegate some activities/responsibilities to the Mobile Command Post(s). The precise nature of the activities/responsibilities and the degree of autonomy bestowed upon the Mobile Command Post(s) would be specific to each application scenario and instantiation of particular emergencies.

Nevertheless, it is important for the system architecture to maintain the communication paths between the Crisis Centre, Mobile Command Posts and Mobile/Static Units.

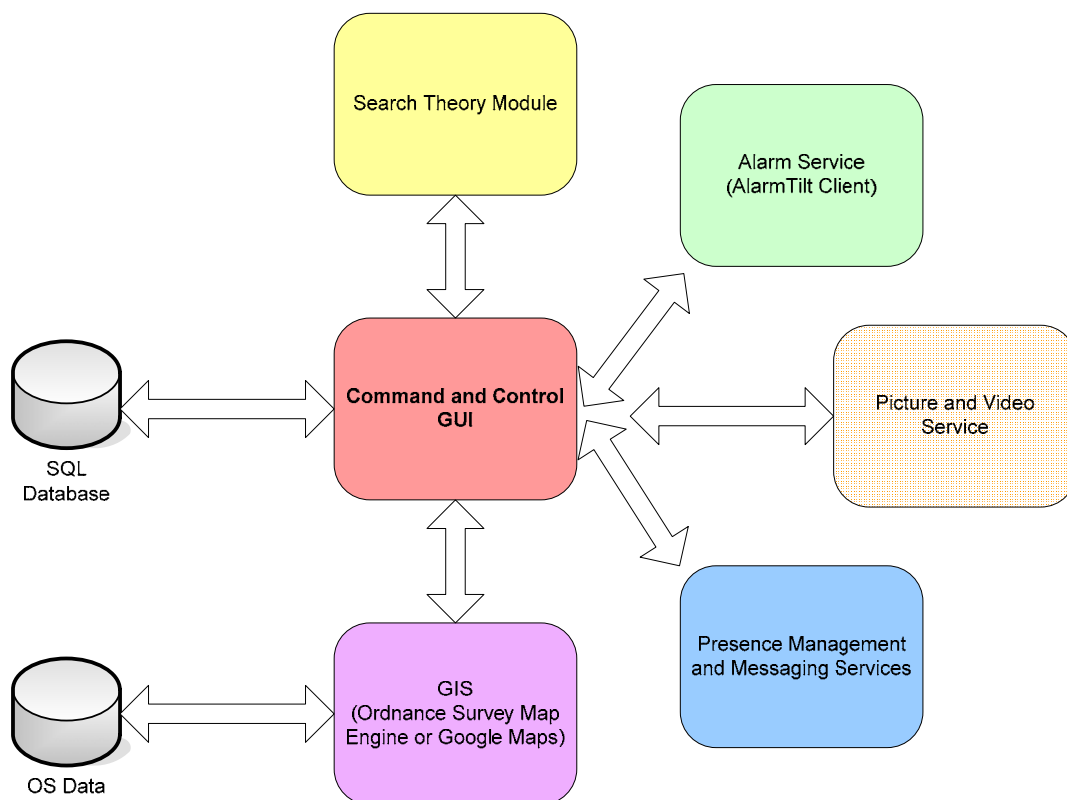


**Figure 8 NSV-4 Crisis Centre**

In the Mountain Rescue scenario, we consider the Crisis Centre to be the headquarters of the Mountain Rescue Team, the Team HQ. The Team HQ is the permanent location from where all the search and rescue operations are organised. The Team HQ contains an Alarm Service to alert team members to emergency callouts (section 4.5), a monitoring service and a directory service (section 4.6). Included in the monitoring service is the presence management service (refer to section 4.4), the picture and video service (section 4.8) and the search theory module (section 4.9).

## 4. Prototype Description / What Has Been Implemented

From a basic perspective, the Mountain Rescue service prototype solution relies on command and control (CaC) software, located at the Team HQ (the Crisis Centre of the u-2010 architecture), to launch, organise, monitor and manage search and rescue operations. The CaC software utilises the software services associated with those features, namely an Alarm Service, Search Theory, GIS, Video and Picture Service, GIS, Presence Management and Messaging Service. Figure 9 depicts an overview of the software that the Team HQ relies on.



**Figure 9 Software Overview**

Complementary to the Team HQ software are the appropriate clients or sources out ‘in the field’, that is, on location in the mountains conducting search and rescue procedures. Mobile devices (PDAs) with each rescue worker provide the hardware to host these software clients (the Mobile Units of the architecture). The Mobile Units are connected to the Team HQ via the networking hardware and software of the IAN and the Mobile Command Posts.

The following sections describe the hardware and software solutions implemented for the Mobile Units, Mobile Command Posts, IAN, WAN, and Crisis Centre subsystems of the u-2010 architecture with respect to the Mountain Rescue service trial.

### 4.1. Satellite and Backhaul Links

The purpose of the satellite and backhaul links is to interconnect the IAN with the global Internet (i.e. the WAN). Since the Mountain Rescue missions are, by their very nature, away from usual communications infrastructure, the ability to connect the IAN rapidly and easily to the global Internet on-demand is of vital importance.

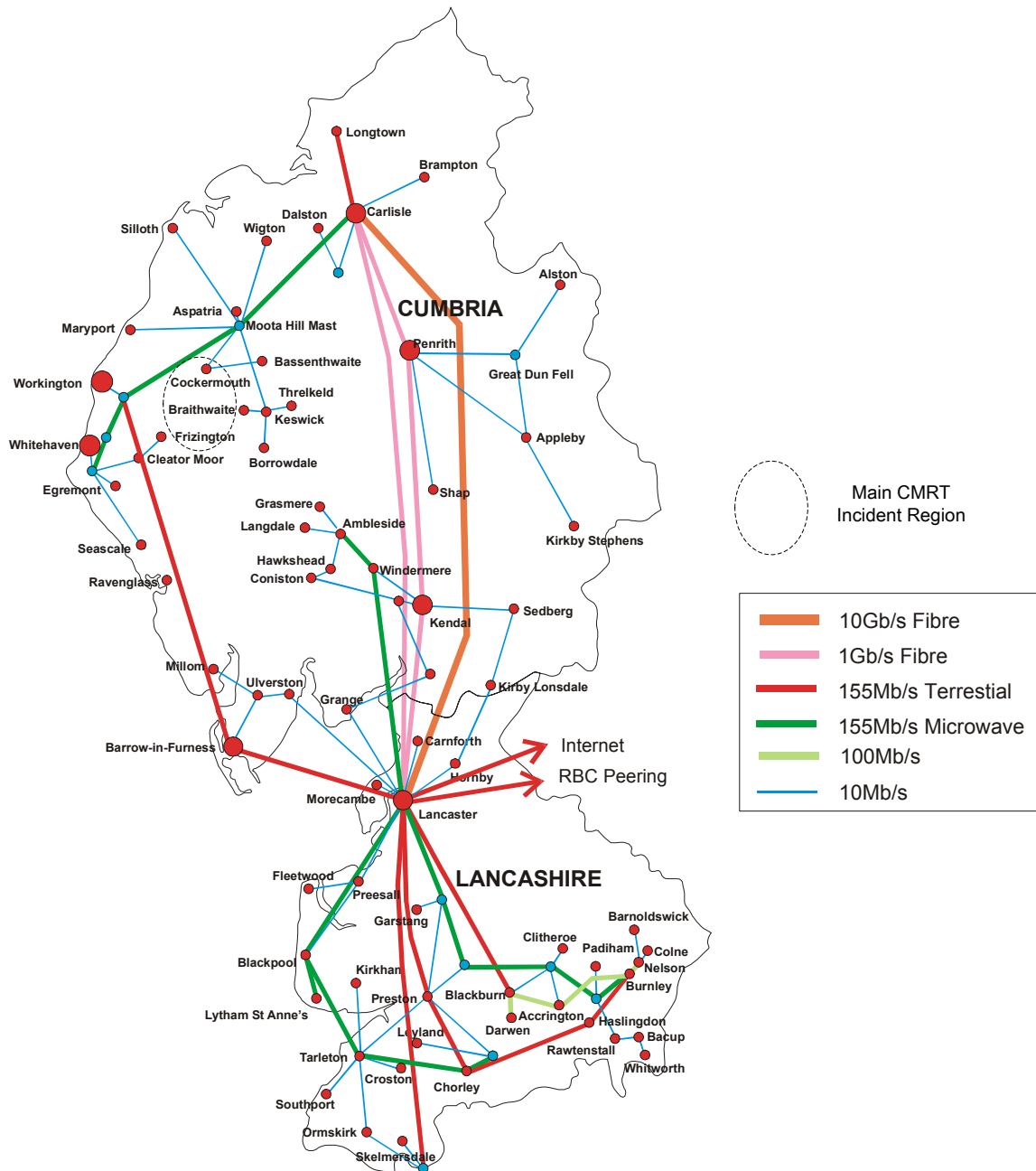


Figure 10 The CLEO Network



Basic IPv4 and IPv6 network services have been implemented in the primary search region of the Cockermouth Mountain Rescue Team. However, this implementation has been fraught with delays and complications throughout the lifetime of the project. Initially, the starting point for deploying network services was to extend from the CLEO network infrastructure. Although the CMRT search region is an extremely rural and sparsely populated area, the CLEO network infrastructure does have some presence in the region.

Figure 10 shows the CLEO network infrastructure running through the counties of Cumbria and Lancashire. It links together over 25 PoPs with a mixture of fibre, wireless and xDSL. The town of Cockermouth itself is served by a 10Mbps terrestrial link to a microwave mast at nearby Moota Hill. In turn, Moota Hill has a 155 Mb/s 5 GHz microwave link to the town of Carlisle, which connects to the CLEO fibre backbone (10 Gb/s).

Yet, although Cockermouth itself is connected to CLEO, the actual search region for the CMRT has little CLEO connectivity, save a DSL connection to Lorton School. For this reason, we had to identify new PoPs that:

1. Were feasible locations for connection to CLEO.
2. Were strategic locations with respect to establishing temporary bases during search and rescue operations.

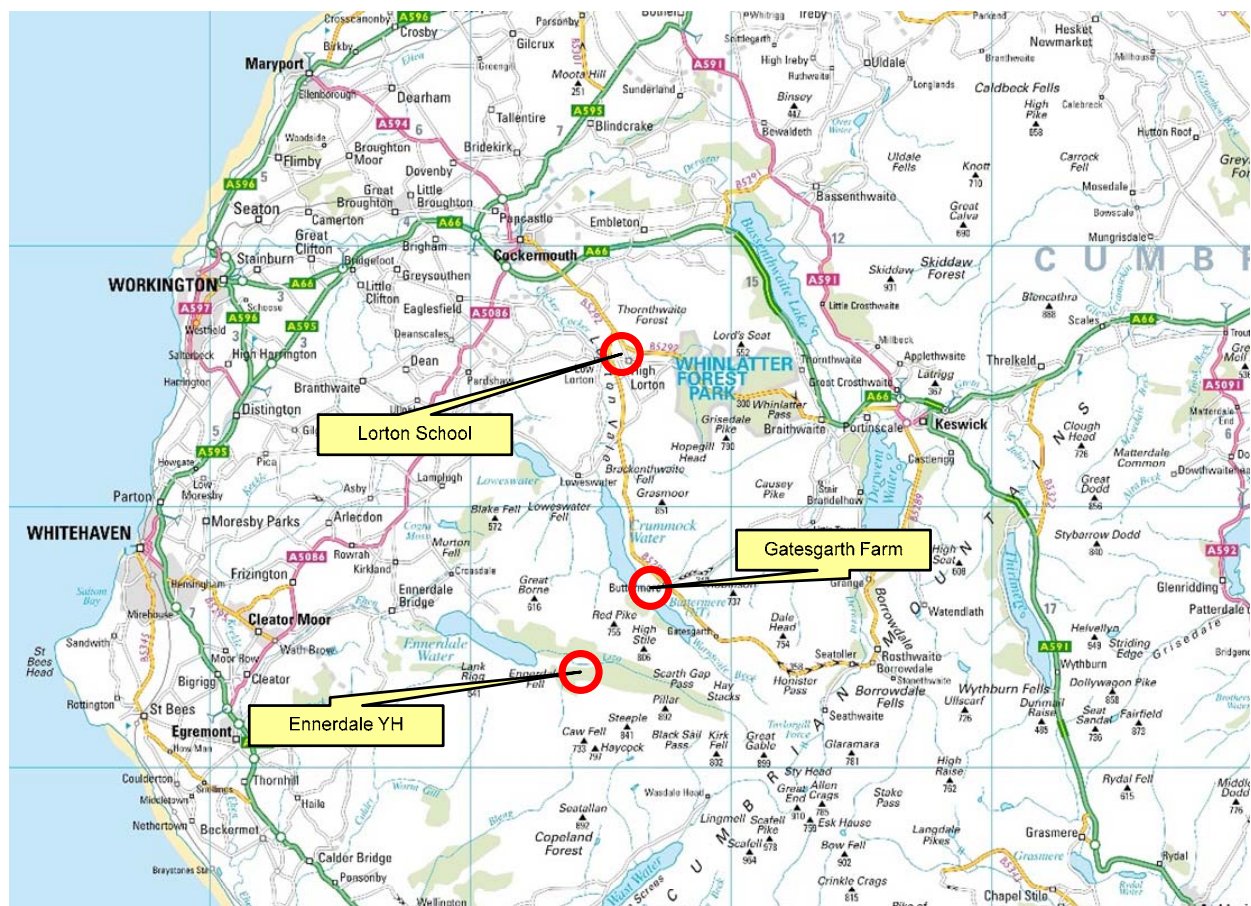
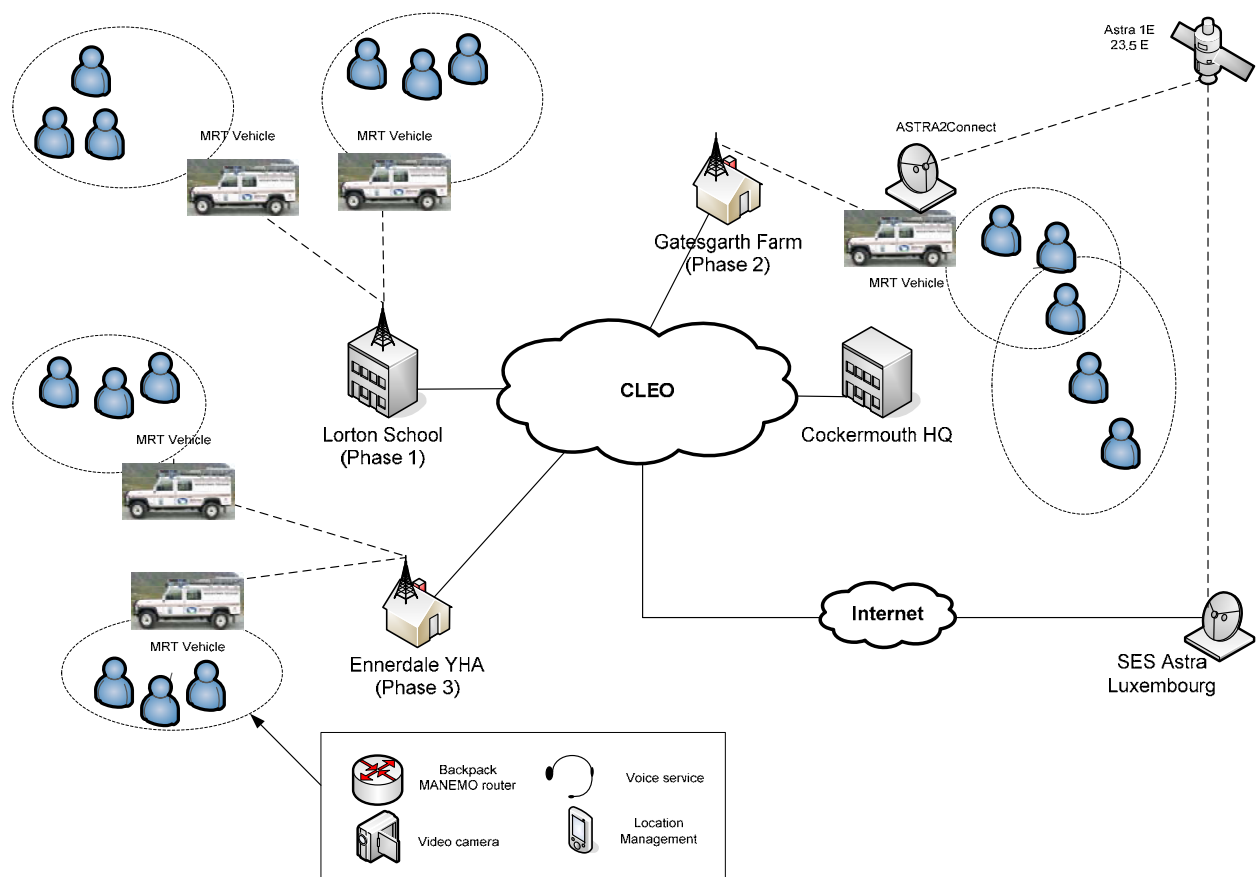


Figure 11 Intended PoP Locations

After much analysis, two new PoP locations were identified in addition to upgrading Lorton School. These PoPs are shown in Figure 11 and are Ennerdale Youth Hostel, Gatesgarth Farm and Lorton School. Both Ennerdale Youth Hostel and Gatesgarth Farm present significant challenges with respect to connecting them to CLEO. The only feasible option is to connect them via DSL, although this would mean installing extra equipment on the roadside between each location and the nearest exchange. The nearest exchange in both cases is over 10 Km away. Although problematic, this was thought to be achievable due to Lancaster University holding ISP status. Both Ennerdale Youth Hostel and Gatesgarth Farm also provide natural locations from which the CMRT can establish command posts from which to conduct their search and rescue operations: these locations have been used many times in the past.


Lorton School on the other hand, is not in an ideal location from which the CMRT can base search and rescue missions. It lies several kilometres north of the most common search locations and is in the lowest part of the area in terms of altitude. However, it was believed that a suitable mast on the roof of the school would enable sufficient line-of-sight (LoS) down the valley to enable a point-to-point link between the school and the base location further down the valley.

In light of these findings, a proposal was made to the CLEO board to establish PoPs at Lorton School, Gatesgarth Farm and Ennerdale Youth Hostel in that chronological order. This also included connecting the CMRT headquarters to CLEO, which from a technical perspective was not problematic. The general network deployment proposed to the CLEO board is shown in Figure 12.



**Figure 12 Envisaged Network Deployment (Longterm)**



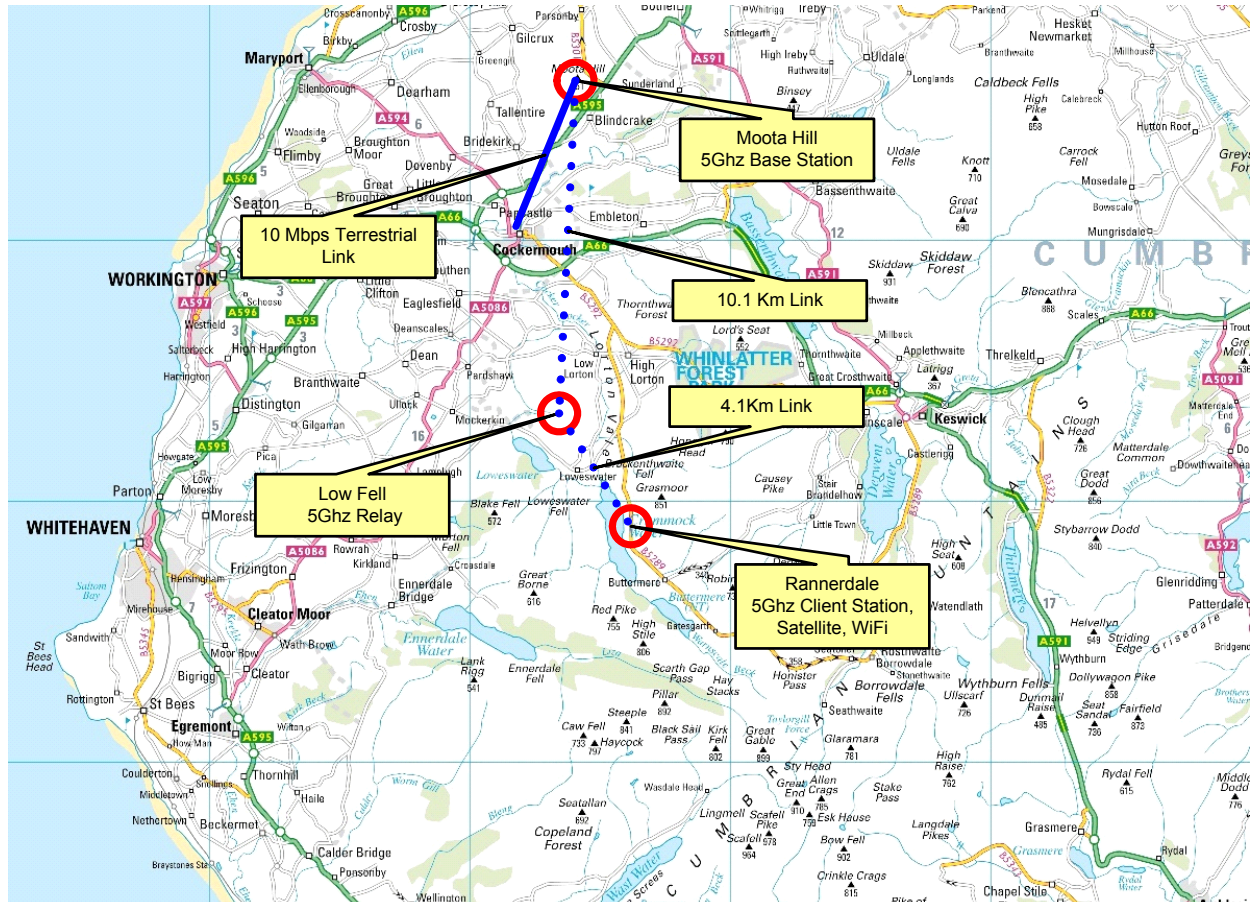
	<h3 style="text-align: center;">D4.2.2 Prototype Mountain Rescue Service Trial</h3>	
---	---	---

Although the proposal was accepted, several bureaucratic delays meant that this deployment will not see the light of day during the lifetime of u-2010. As a result, we re-evaluated our deployment options and came up with a different strategy.

Realising that we were unlikely to secure permanent PoPs for CLEO within the lifetime of the project, we implemented temporary ‘rapid-response’ PoPs that could take their place. The idea behind these PoPs was that either a rescue vehicle or a couple of rescue workers could quickly establish a temporary PoP by setting up wireless point-to-point or point-to-multipoint links with known permanent PoPs elsewhere. For this reason, the equipment that comprises the rapid-response PoP needed to be as compact and lightweight as possible so that it could be easily carried by one or two rescue workers. An added advantage of the rapid-response PoP is that it can be used in other emergency/crisis scenarios to provide backhaul links on-demand where there are ‘black holes’ in wireless coverage.

For the Mountain Rescue scenario, the rapid-response PoPs would quickly establish a 5 GHz point-to-point link with the Moota Hill mast, just north of Cockermouth. We identified several key locations where good line-of-sight to Moota Hill offers excellent relaying possibilities to search bases. Perhaps the best location for this is Low Fell to the north of Crummock Water, as Low Fell offers good LoS to Moota Hill in addition to key car park locations and popular tourist locations from which relay points can be placed.

Figure 13 illustrates the key locations of the mountain testbed. We use the car park at Rannerdale Farm, on the East shore of Crummock Water as the base for a search and rescue operation. At this location, we construct the IAN by establishing a Wi-Fi hotspot that is directed towards the search area into which the rescue workers are moving. Of course, backpack mobile routers that run MANEMO, should ensure connectivity remains between rescue workers even when they move out of range of the hotspot. Uplink to the Internet from the base location is provided by a satellite connection and a radio link to CLEO.



**Figure 13 Testing Locations within the CMRT Search Region**

The satellite connection uses the Astra2Connect satellite service and connects to the Astra 1E satellite at 23.5°E. The link to CLEO consists of a 5 GHz microwave relay that begins at the car park and is relayed from Low Fell to the Moota Hill mast. The distance of the Rannerdale car park to Low Fell leg of the link is 4.1Km. The Low Fell to Moota Hill leg of the link is 10.1Km.

Figure 14 shows the 5 GHz relay established on Low Fell, with Figure 15 showing the Rannerdale car park end of the radio link. Both ends of the link can be established in as little as five minutes after arrival at the location. Of course, rescue workers must carry the Low Fell relay equipment in their backpacks, which is a disadvantage, but we have managed to keep the total backpack weight below 5 Kg (about the same weight as two average size laptops). This combination of relatively low backpack weight and quick link establishment allows the rapid-response PoP to become a realistic solution.



Figure 14 5 GHz Radio Relay on Low Fell



Figure 15 5 GHz Radio Link at Rannerdale



At the Rannerdale car park location, we use an 18dBi directed antenna for the mountain ‘hotspot’. This antenna has a vertical radiation pattern of  $45^\circ$  and a horizontal radiation pattern of  $75^\circ$ . From this location, this allows us to cover the entire West side of Grasmoor (a popular mountain) with one antenna. Of course, it is possible to add more antennas to the mounting to create multiple sectors of coverage.

Regarding the Astra2Connect satellite connection, we initially had some problems in establishing the connection with the satellite. High-winds can often disrupt the synchronisation with the satellite as the dish has a tendency to move regardless of how securely it is fixed to its mounting pole. However, once the satellite receiver is synchronised, the connection remains stable even in the presence of high winds. On average, the satellite connection can be established within five minutes of reaching the location. Although the Lake District is on the edge of the satellite coverage footprint, we achieved an average downlink rate of around 990Kbps and an average uplink rate of around 244 Kbps in our tests. Round-trip times between the mountain location and Lancaster University (thus traversing Luxembourg and GEANT) averaged at around 600ms. When using IPv6, an IPv6-in-IPv4 tunnel was established using the Hurricane Electric tunnel broker service [15], and round-trip times increased to around 1000ms.



**Figure 16 Astra2Connect Link with Grasmoor in Background**



**Figure 17 “Communications Vehicle”**

One of the major requirements of the satellite link and rapid response backhaul PoPs, was to keep bulk and weight down to a minimum. Ideally, all the communications equipment needed for a search group should be self-contained within the rescue vehicle(s) assigned to that group. In general, all the communications equipment and generator can fit into an average family sized hatchback car (Figure 17). Only the size of the Astra2Connect satellite dish can sometimes cause problems, as this is 80cm in diameter. It may be possible to use a smaller diameter satellite antenna if connecting to other satellite broadband services. However, even an 80cm dish antenna can be easily stowed on the roof assembly of a typical rescue vehicle.

## 4.2. Backpack Routers

In the Mountain Rescue scenario, the backpack routers are a fundamental component of the overall solution. The backpack routers are small, lightweight, multi-interfaced mobile routers, specially developed to form the main part of the IAN in search and rescue missions. Their primary role is to run the MANEMO protocol suite (see following section) to maintain connectivity between the rescue workers and the IAN as the search groups roam away from their command post. In situations where no connection to the IAN is possible, the backpack routers can also provide their own Internet gateway if suitable GPRS/UMTS coverage is available. They can also provide a secondary role as a sensor gateway, if 802.15.4 sensor hardware is deployed.

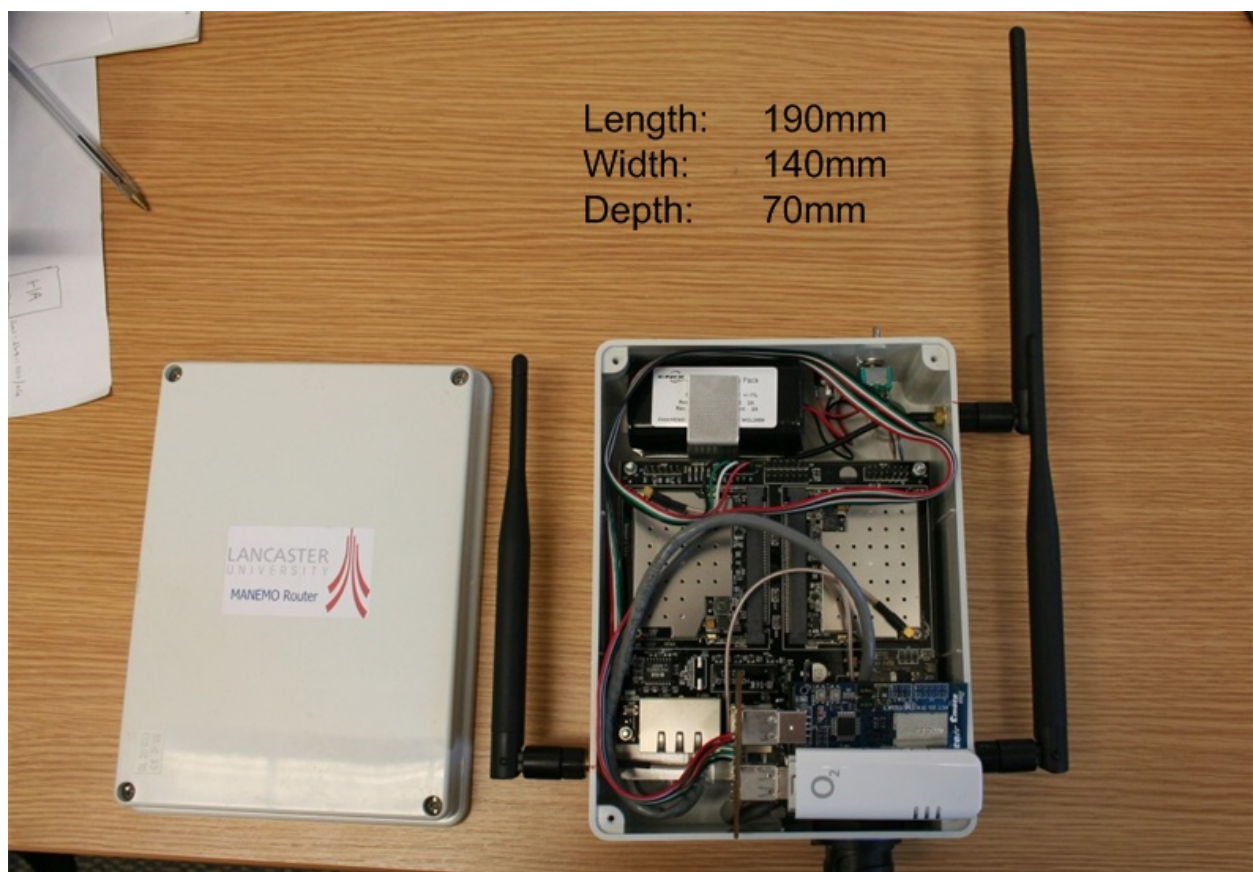
The backpack routers have been designed and developed at Lancaster University specifically for u-2010. The main boards we are currently using for the backpack routers are Ubiquiti Routerstations [17]. After much analysis and testing, this was considered the best board for all our requirements (size, weight, performance, radio capability and Linux-compatibility). There are other board possibilities (e.g. Gumstix, mini-ITX, ALIX, Gateworks) but they are inferior to Ubiquiti boards with respect to one or more of our



requirements. We only considered single-board computers (SBCs) and ruled out PC-104 based boards due to their size and layout resulting in a relatively large enclosure.

The Routerstation board can only be powered via the power-over-Ethernet (PoE) port so inside the router enclosure we have a simple circuit that connects a Lithium-Ion battery to the PoE port. The board accepts anything between 12-24V, although our tests with numerous 12V batteries were unsuccessful as they would sometimes drop their supply below 12V. The Lithium-Ion batteries we use are 15V and supplied by Enix Energies; anything higher than 15V and the batteries we found were too big and heavy for a backpack router.

The Ubiquiti Routerstation boards have three mini-PCI slots and so each backpack router contains three Wi-Fi modules. These Wi-Fi modules are Ubiquiti XtremeRange2 (2.4 GHz) and XtremeRange5 (5 GHz) which can be exchanged according to requirements. We use one Wi-Fi module for the PAN, one module for MANET connections and one module for connecting to access points. Each Wi-Fi module is connected to a dual 2.4/5 GHz omnidirectional antenna giving 5dBi gain. On the outside of the enclosure, there is a bare minimum of features in order to simplify user operation. An on/off switch is accompanied by a charger socket and an Ethernet connection is provided to allow the backpack router to be connected to other devices across a wired LAN.



**Figure 18 Inside the Backpack Router**

We have also integrated a GPRS/UMTS module and a TMote sensor board via a small form-factor USB hub that connects to the USB port of the Ubiquiti main board. The GPRS/UMTS capability is important for maintaining global Internet connectivity when there is no global route via any of the 802.11 interfaces.

An intelligent software module for handover management (described in the following section) is able to determine when this interface should be used. The integration of the TMote sensor board allows the backpack router to also function as an 802.15.4 gateway and thus provide seamless sensor networking in a mobile environment. Figure 18 shows a photo of the inside of a backpack router.



**Figure 19 Backpack and Router**



**Figure 20 Backpack Router worn by Rescuer**

The enclosure of the backpack router is IP56 rated, made of thermoplastic and is resistant to water, heat and minor shocks. The dimensions of the backpack router (excluding antennae) are 190mm x 140mm x 70mm (length x width x depth).

The total weight of the backpack router (including the GPRS/UMTS module and TMote board) is only 1.2Kg, much less than an average laptop (circa. 2.5Kg) and around 8% less than typical netbooks such as the Samsung NC10 (1.33Kg) and the Asus Eee PC (1.3Kg). Since the rescue workers must carry their usual (and often heavy) non-communications related equipment on search and rescue missions, the added size and weight of a mobile router could be extremely unwelcome.

Fortunately, the relatively small size and light weight of the enclosure means that it can easily fit inside the pouch of a backpack. The enclosure was designed so that the omnidirectional antennae would be vertical when placed inside the backpack to maximise the efficiency of the antennae's horizontal polarisation. However, Ubiquiti are due to launch a new board, the RouterStation Pro [18] which has a few improvements including a power jack, USB housing, SDIO and serial port, although it will be slightly larger and may require a redesign of the enclosure.

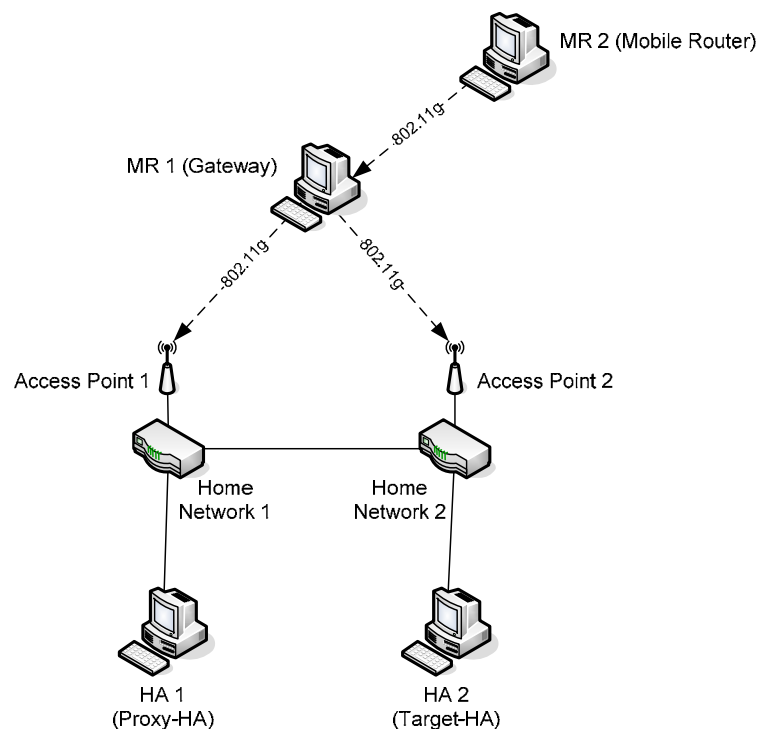
### **4.3. MANEMO**

Both flavours of MANEMO, namely NEMO-Centric and MANET-centric have been implemented within one software architecture, dubbed the Unified MANEMO Architecture (UMA).

From an early stage, it was deemed it important to develop a working experimental implementation of UMA rather than simply produce simulations of the overall process, in order to realise a working solution that could be deployed and tested in real scenarios.

Development of the UMA suite of protocols was carried out on a collection of four standard specification x86 PCs running the Linux Operating System. To facilitate the protocol development, each of these PCs was assigned a separate individual role during the initial implementation phase and then finally, once completed the software implemented across each of these machines was merged to produce one single instance of each of the UMA software components. The roles of the testbed machines correlated to the four possible roles that can arise in the UMA model, namely Target Home Agent (HA), Proxy Home Agent (Proxy-HA), Mobile Router (MR) and Gateway Mobile Router (Gateway). In addition to the machines that development was performed upon, the UMA development testbed also incorporated two static routers, which provided two separate home networks (on which the HAs resided) and multiple wireless enabled foreign networks.


An illustration of the development testbed is provided in Figure 21, each of the MRs used in this setup contained multiple Ethernet network interfaces (to support wired communication with attached hosts as well as two Wi-Fi network interfaces capable of supporting 802.11a/b/g in either ad-hoc or infrastructure mode).



**Figure 21 UMA Prototype Development Testbed**

Each of the HAs contained one Ethernet interface, which was used to connect the HA to the Home Network Access Router. The UMA protocol development was performed on PCs running the Ubuntu Linux distribution (Version 7.10) with version 2.6.22 of the Linux kernel. All of the implementation code was written in ANSI C using the Kdevelop development environment and was compiled using GCC version 3.1.



	<h3 style="text-align: center;">D4.2.2 Prototype Mountain Rescue Service Trial</h3>	
---	---	---

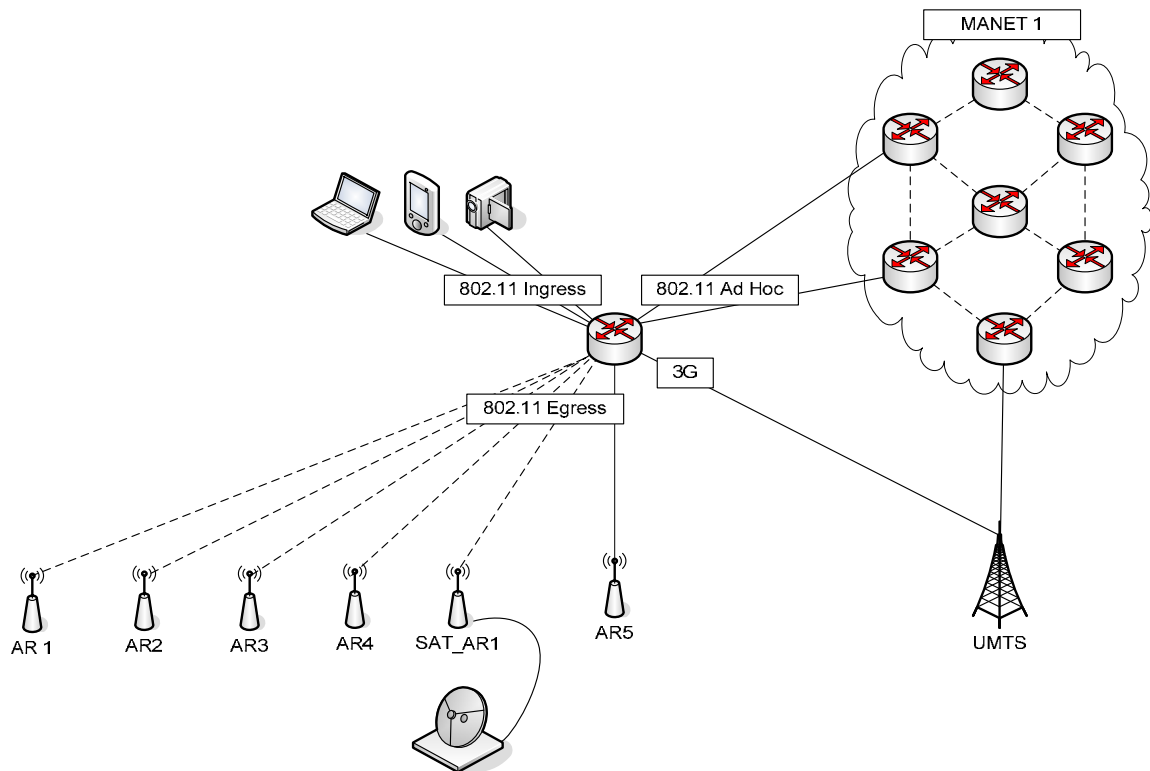
In order to provide a more suitable platform for deployment on small form-factor hardware, the UMA software was ported to OpenWRT Kamikazee and has been successfully tested with the Ubiquiti Routerstation board (see previous section) and the Linksys WRT54G router. This is especially useful for deploying small, compact mobile routers such as the backpack router used in the Mountain Rescue scenario.

For further details on the implementation and evaluation of the UMA, please refer to D2.2.2 Report on u-2010 Mobility Solution [4].

#### 4.3.1. Intelligent Handover Management

A Mobile Router (MR) should be an autonomous entity, capable of operating continuously without any manual interaction from an end user. A MR running UMA can conceivably adapt to the changing topologies of the IAN and ensure that the best possible network layer routing is always utilised. However, whilst the network protocols running on the MR are able to adapt to such changes in the network, they do not actually *trigger* any changes (i.e. network handovers) to occur in the first place. The types of changes we refer to are those related to utilising the best possible connection to the Internet at any given time. For this, we have implemented a utility that is auxiliary yet complementary to the UMA network protocols, which we call the Handover Manager. The Handover Manager's role is to constantly monitor all of the available connectivity options and intelligently decide the most appropriate connection to the Internet to utilise.

Figure 22 illustrates a typical scenario the Handover Manager may be presented with. In this diagram, the Mobile Router is currently connected to the Internet via the Wi-Fi access point AR\_5. As an alternative, it can also choose to communicate with nodes in the Internet via a UMTS connection it has in place, via its ad-hoc interface connection with MANET 1, or it could choose to establish its Wi-Fi connection with another alternative access point (AR\_1, AR\_2, etc). If the connection that the MR has in place with AR\_5 is satisfactory, then it will continue to be utilised. However, if the MR's connection with this access point becomes weak and its throughput drops below a satisfactory level, then the Handover Manager will intervene by establishing a connection with a more suitable alternative.

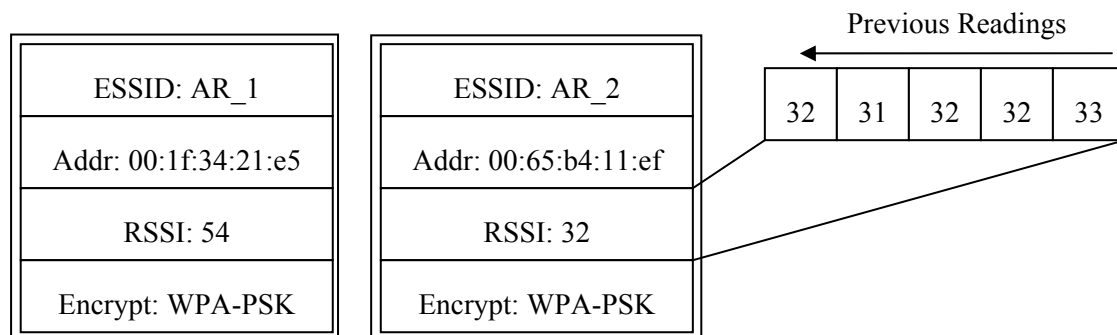


**Figure 22 Connectivity Option Example**

In order to determine the most suitable alternative from the connectivity options, the Handover Manager simultaneously monitors a number of parameters:

- Signal strength of all appropriate Wi-Fi access points in range.
- Layer 3 connectivity of its current Wi-Fi connection (if present).
- Layer 3 connectivity of its UMTS connection.
- Availability of a gateway in any MANET it is connected to.

Only Wi-Fi access points that the Handover Manager is configured to accept are deemed “appropriate” connections. However, configuration of the Handover Manager can support coarse and fine-grained specification of access points and their characteristics. This can range from allowing the MR to connect to any openly available access point, through only permitting it to connect to access points that match certain SSIDs, to connecting only to specific individual access points identified by their MAC address. If an access point that matches the outlined specifications comes into range, the Handover Manager creates a record and stores information about it for the remaining time it is visible. In addition to the static information related to the access point, the Handover Manager also periodically updates the Received Signal Strength Indicator (RSSI) value it has recorded for the access point and then stores the previous *n* results in a sub-table.



**Figure 23 Access Point Information**

The availability of Layer 3 connectivity for both the current Wi-Fi connection and the UMTS connection is monitored by periodically transmitting ICMPv6 Echo Request packets to the Home Agent. When the Handover Manager is first started it communicates with the UMA protocol, learns the HA's address and then begins transmitting. The Handover Manager sends requests directly to the HA because if the full path all the way to the HA in the Home Network is not available then the connection is deemed not usable and an alternative must be selected.

For any connection to a MANET of other mobile nodes, the Handover Manager determines its suitability for use as an Internet connection by monitoring for the availability of a Gateway node. If a Gateway is present in the MANET and is usable by the MR, then it will periodically receive advertisements from the Gateway. The Handover Manager checks for continuous receipt of these advertisements and updates the status it records for the MANET connection if these advertisements stop arriving.

At present, the Handover Manager uses a simple connection preference model:

1. Wi-Fi Internet access network.
2. UMTS.
3. Wi-Fi extension of satellite connectivity.
4. MANET with visible Gateway.

Any appropriate Wi-Fi network that provides a direct connection to the Internet is selected first. If no access points matching this criterion are available, the Handover Manager first checks the current status of the Layer 3 connectivity of the UMTS connection (this information is immediately available to the Handover Manager because it periodically checks the UMTS connection at all times in parallel to its other operations). If the UMTS connection is unavailable, the next connection the Handover Manager will consider is an access point that offers an indirect link to a satellite access network. Finally, if no satellite connection is available either then the connection with a MANET will be utilised if a suitable Gateway is present. Finally, if no connectivity options are available at all, the Handover Manager will not perform any handover and will instead continue to monitor all interfaces for the first available connection.

#### **4.4. Presence Management and Messaging Services**

The presence management service (PMS) developed at Lancaster University identifies and monitors the presence or location of emergency workers and vehicles in emergency scenarios, following the presence management definition given in Section 1.1, D3.2.1 Report on the Presence Management Solution [5]. Using the PMS, the mission coordinator of a rescue team can keep track of the rescue workers during a mission, and also keep a broad picture of the search and rescue operation. This helps the coordinator to

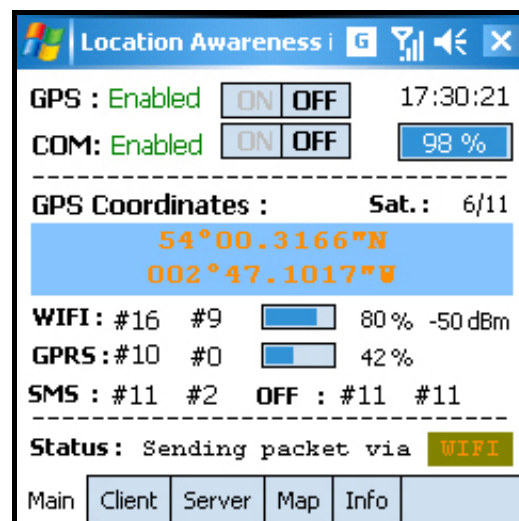
make informed decisions and increases the efficiency of the rescue team. The PMS can be used before, during and after an emergency operation according to the needs of the emergency organisation using it. The PMS consists of a number of PDA devices that periodically transmit location updates to a server application located at the rescue team's headquarters. The client and server applications are also capable of transmitting text messages to/from each other. Using this feature the mission controller can inform the rescue workers of important information during the course of the search and rescue operation. Conversely, the rescue workers can bring important information pertaining to their searches to the attention of the mission controller. These messages can take the form of instant messages over the IPv6 network and/or SMS messages using the GSM network.

The client application has been designed and implemented to run on any Windows Mobile 5.0 (or higher) device having WI-FI, GPRS and GSM capability. Ideally, the GPRS module of the client device should be class A so that the client application will be able to use GPRS and send SMS at the same time. However, PDA devices that have a GPRS module of class B were found to be sufficient, if not ideal.

Regarding the acquisition of the GPS coordinates, the client device can have either an internal GPS module or be able to obtain coordinates from an external GPS module over Bluetooth.

The client application includes five different tab-pages:



1. Main - the main screen of the application.
2. Client - for settings regarding the client.
3. Server - for settings regarding the server.
4. Map - for displaying a map to the rescue worker showing his/her location.
5. Info - information obtained from the GPS satellites.



**Figure 24 Main Tab of Client Application**

The Main tab, depicted in Figure 24, is the main screen that the mountain rescue worker sees during a mission. This screen presents information about:

- the rescue worker's location
- the number of GPS satellites that the application can lock and view

	<h3 style="text-align: center;">D4.2.2 Prototype Mountain Rescue Service Trial</h3>	
---	---	---

- indications for the Wi-Fi and GSM signal strength
- the current connectivity option being used
- the statistics for the messages being sent according to each connectivity option.

The client application can also display the walking speed of the rescue worker holding a device or the driving speed of a vehicle that the rescue worker is in, based on data retrieved from the GPS module.

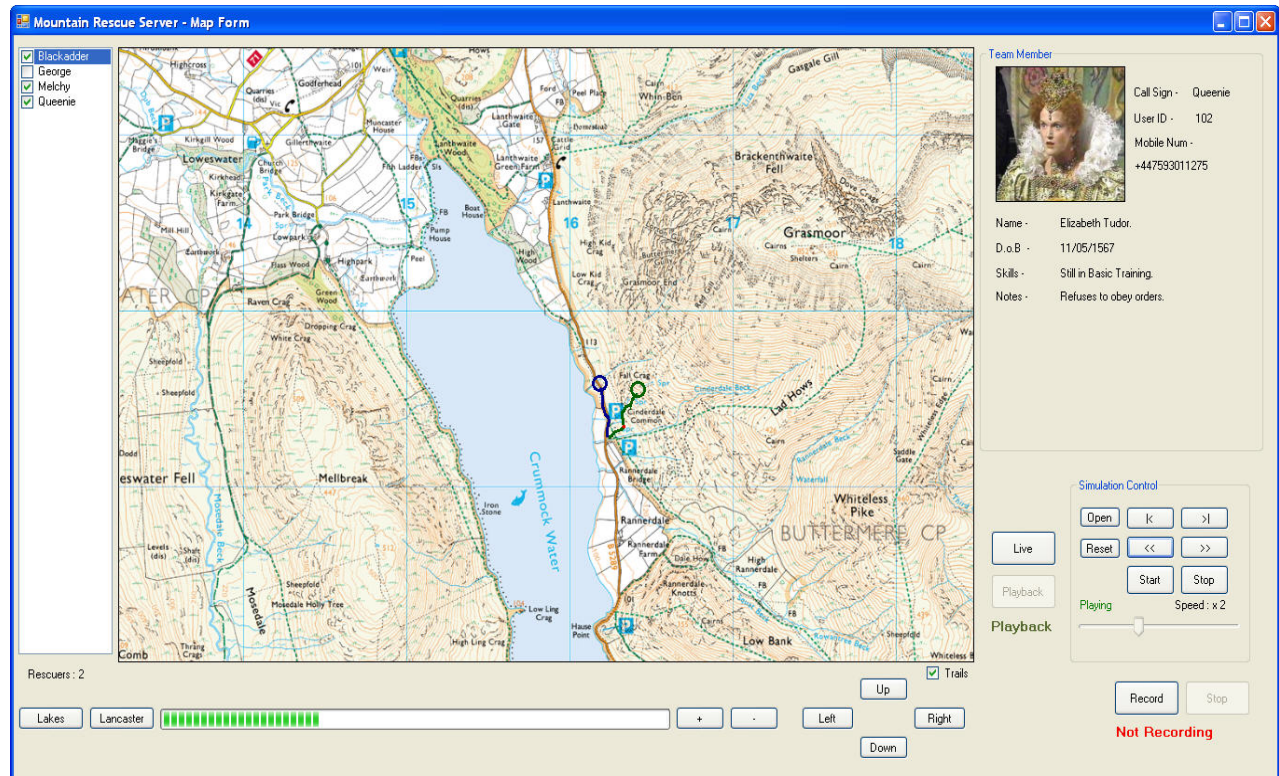
The client application has been successfully used on the following PDA devices:

- HP IPAQ 6915 (Intel PXA270 416Mhz CPU, 128 MB ROM and 64 MB SDRAM, Windows Mobile 5.0, Wi-Fi 802.11b, GSM/GPRS/EDGE, Bluetooth)
- HP IPAQ 914c (Marvell XScale PXA270 520MHz CPU, 128 MB ROM and 128 MB RAM, Windows Mobile 6.1, Wi-Fi 802.11b/g, HSDPA/UMTS, GSM/GPRS/EDGE, Bluetooth, GPS)
- HTC Touch Cruise (Qualcomm MSM7200 400MHz CPU, 256MB ROM, 128MB RAM, Windows Mobile 6.0, Wi-Fi 802.11b/g, HSDPA/UMTS, GSM/GPRS/EDGE, Bluetooth, GPS)
- HTC Touch Cruise T4242 (Qualcomm MSM7225 528MHz CPU, 512MB ROM, 256MB RAM, Windows Mobile 6.1, Wi-Fi 802.11b/g, HSDPA/UMTS, GSM/GPRS/EDGE, Bluetooth, GPS)

The client application ran successfully in all the aforementioned devices, observing a better performance on the IPAQ 914c and both HTC Touch Cruise models, which are more recent, higher-specification devices running Windows Mobile 6.0 or later.

The main aim of the server application is to listen for incoming messages being sent from the PMS clients, regardless of which network the client used to transmit the messages. The server application processes the payload of each arrived message and plots the received GPS coordinates of the rescue members onto a map to assist the mission coordinator in tracking the progress of a mission and take informed decisions. The locations of rescue workers are updated on the map in real-time in response to the location updates being sent by the clients.

A screenshot of the PMS server application is shown in Figure 25.



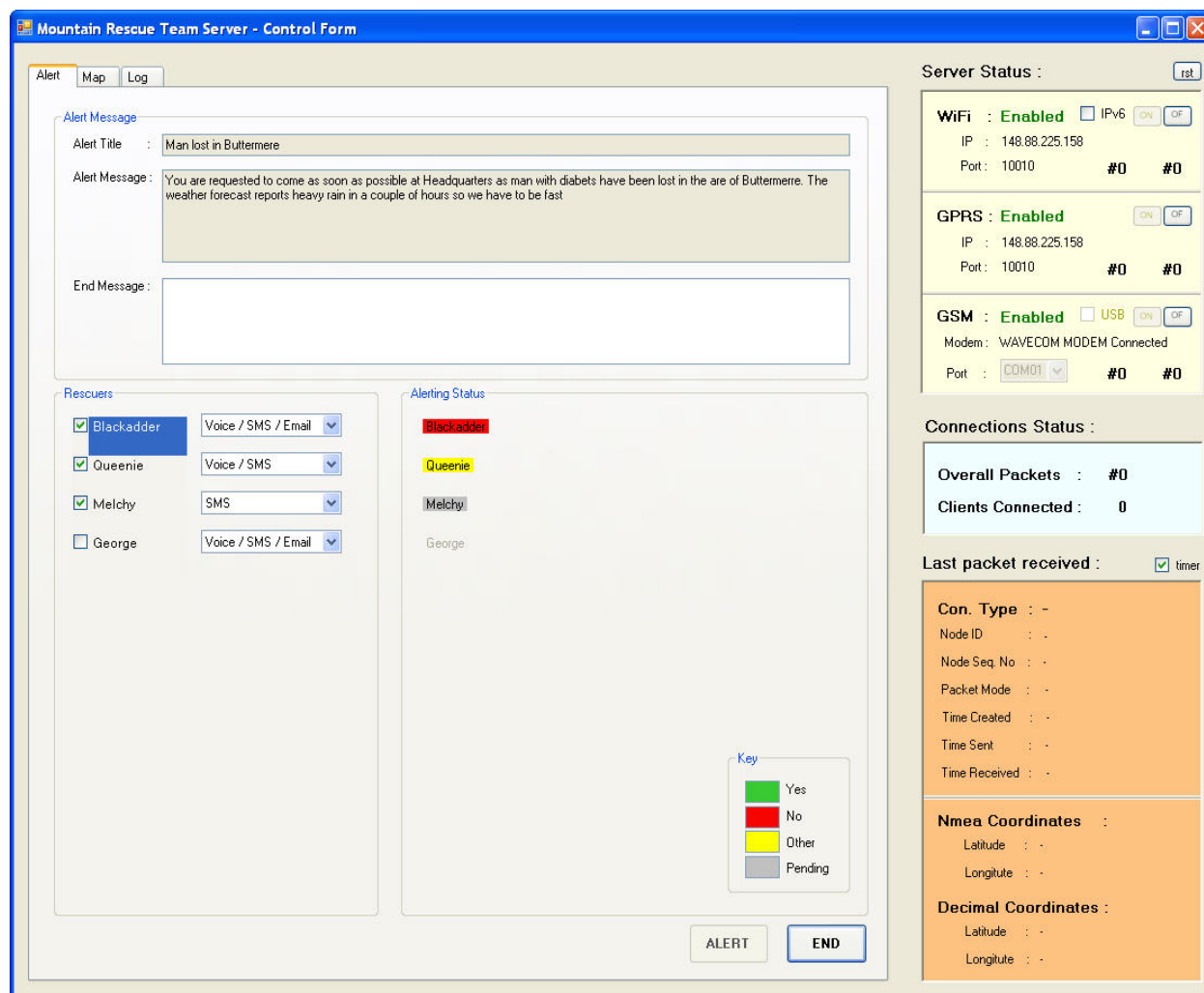
**Figure 25 Screenshot of the PMS Server Application**

A detailed investigation of the PMS design and implementation is provided in Deliverable 3.2.1, Report on the Presence Management Solution [5]. A description of the necessary hardware and software requirements and instructions for configuration and usage are available in D3.2.2, Prototype of the Presence Management Solution [6].

## 4.5. Alarm Service

An Alarm Service for the Mountain Rescue scenario has been implemented using M-PLIFY's AlarmTilt service (see deliverable D4.1.1, Prototype of an alarm and emergency communication system based on the developed architecture and services in Luxembourg [7]). Using a modified version of the AlarmTilt SOAP API we have implemented a system that alerts rescue workers to emergency calls and replaces (or is complimentary to) the current paging system. Messages can be sent via email, SMS, voicemail or a bespoke client-server messaging system. This functionality is integrated into the server application of the PMS. Figure 26 shows a screenshot of the PMS server with the Alert tab (containing the AlarmTilt client functionality) active.





**Figure 26 Screenshot of the Mountain Rescue Alarm Service using AlarmTilt**

From this page, the mission coordinator can launch an emergency, contact the selected rescue workers, and monitor their responses. The rescue workers that respond to the emergency are automatically displayed on the map page once their location updates begin to be received.

For more information regarding the integration of the PMS and AlarmTilt, please refer to Report on the Presence Management Solution [5].

## 4.6. Directory Service

Directory Services have not been implemented for the Mountain Rescue scenario. Instead, the PMS and other services consult an SQL database via the CaC component (Figure 9) to gain information about rescue workers, their devices and previous incidents. The SQL database is implemented using MySQL v5.0.67.

Some of the more important table schemas are described below.

**Table 2 - Members Table Schema**

Field	Type	Null	Key	Default	Extra
id	varchar(16)	NO	PRI	NULL	
firstname	varchar(64)	NO		NULL	
surname	varchar(64)	NO		NULL	
callsign	varchar(16)	YES		NULL	
mobile_tel	varchar(32)	YES		NULL	
home_tel	varchar(32)	YES		NULL	
work_tel	varchar(32)	YES		NULL	
email	varchar(64)	YES		NULL	
home_addr	varchar(128)	YES		NULL	
dob	date	YES		NULL	
skills	varchar(128)	YES		NULL	
notes	varchar(1024)	YES		NULL	
photo_url	varchar(512)	YES		NULL	
available	char(1)	YES		y	
security_code	varchar(32)	YES		NULL	

Perhaps the most important information in the ‘members’ table is the contact details for each team member and whether they are available to respond at the present time. This information is used by the Alarm Service component to alert available team members when an emergency call is triggered.

**Table 3 - Devices Table Schema**

Field	Type	Null	Key	Default	Extra
id	varchar(16)	NO	PRI	NULL	
member_id	varchar(16)	YES	MUL	NULL	
device_desc	varchar(128)	NO		NULL	
sn	varchar(64)	YES		NULL	

When the PMS clients begin to transmit location updates to the PMS server, the CaC module can determine the team member associated to each client device by consulting the ‘devices’ table of the database.



**Table 4 - Incidents Table Schema**

Field	Type	Null	Key	Default	Extra
id	int(10) unsigned	NO	PRI	NULL	
start_time	datetime	NO		NULL	
finish_time	datetime	YES		NULL	
location_gps_lat	varchar(16)	YES		NULL	
location_gps_long	varchar(16)	YES		NULL	
location_desc	varchar(512)	NO		NULL	
incident_desc	varchar(2048)	NO		NULL	
injuries	varchar(512)	YES		NULL	
log_url	varchar(512)	YES		NULL	

The ‘incidents’ table of the database is extremely important as it holds vital information pertaining to every search and rescue mission. This includes that start and finish times of the mission, the location where the casualty was found, details of injuries and a link to where the mission log can be found. The mission log is used by the command and control software to replay missions.

**Table 5 - Incident\_Rescuers Table Schema**

Field	Type	Null	Key	Default	Extra
incident_id	int(10) unsigned	NO	PRI	0	
member_id	varchar(16)	NO	PRI		
notes	varchar(512)	YES		NULL	

Further to the information contained in the ‘incidents’ table, the ‘incidents\_rescuers’ table details all the team members involved in each rescue mission along with any notes pertaining to the performance of the team members on each mission.

## 4.7. Voice Service

For the Voice Service, a bespoke VoIP system purely for the Mountain Rescue personnel was designed and implemented at Lancaster University.

The motivation behind the voice service is to provide an alternative means of voice communication than 2-way radio or mobile phones for keeping members of a Mountain Rescue team in contact. Members of such a team would require to be kept in constant voice communication with each other and possibly, with

other Mountain Rescue teams in the area. It can be ineffective to use more traditional means of communication, such as mobile phones or radios, for two reasons:

1. Coverage – In mountainous areas, GSM signals are unreliable, even if a call is established, a cutout in signal will mean the call is dropped and the user has to dial again. 2-way radios tend to have much better coverage although even this is less than 100%.
2. Cost – The expense of purchasing a frequency for 2-way radios is considerable for a charity-based Mountain Rescue team. Mobile phones tariffs are much cheaper, although still unrealistic for the Mountain Rescue team to fund the bills for each rescue worker.

By using a VoIP service over the ad-hoc IAN infrastructure created by the rescue workers and vehicles, these cost issues become less significant. Unfortunately, a CoTS VoIP system is not sufficient in this scenario since they depend on constant connectivity to the backend infrastructure (e.g. VoIP servers and SIP gateways), making them unreliable. Reliability is an essential part of Mountain Rescue communications and only a system that is dependable can be used in search and rescue missions. Therefore, cutouts in network connectivity *must not* result in dropped VoIP calls (both one-to-one and group). In simple terms, the voice communication must be transmitted on a best effort basis and with no teardown of call state if there are network problems. Due to the terrain, wireless signals can fluctuate rapidly in the short term, yet can show quasi-stability in the long term.

For these reasons, a bespoke VoIP system purely for the Mountain Rescue personnel is necessary. The VoIP clients are designed to run on any Windows Mobile PDA device and they have been successfully tested with the following hardware: HP iPAQ 6915, HP iPAQ 914 and HP iPAQ 6315 and HTC Touch Cruise.



**Figure 27 Simple Large Button GUI for Voice Service Client**

Due to the harsh conditions faced by the teams, they usually wear protective clothing such as gloves. This necessitates a GUI with large, easily accessible buttons to operate the voice service. Moreover, the GUI needs to be simple, intuitive and uncomplicated so not to detract from the normal search and rescue operations that have to be performed (Figure 27).

Several bespoke features within the VoIP application specifically target the Mountain Rescue domain. One of these is the optional push-to-talk mode that works in a similar way to that of a conventional

	<p align="center"><b>D4.2.2 Prototype Mountain Rescue Service Trial</b></p>	
---	---	---

handheld two-way radio system. Using this mode, only one user can speak at any one time. This is achieved through the use of a token passing system that is integrated as part of the inter-device communication system. The token passing system works by sending communication messages pertaining to a single token, which is required by the client application to allow transmission of audio data. The token is a flag that is used to represent whether the application has transmission control. Only one token should ever exist in a group; there are several safeguards to ensure that multiple tokens do not exist.

Groups can be defined and associated with one toggle button, allowing easy transmission to a certain group of users (e.g. all medics). Another useful feature is the user blackout option, which is designed so that conversations can be limited between certain users within the team. The buttons on the GUI have the name of all other users in the group and either ON or OFF labelled next to them. In a larger group, this would allow transmission to a desired selection of users with unselected users not hearing the transmission. With smaller groups, this can be used for one-to-one or n-way transmissions.

In order for the VoIP clients to discover each other, we have implemented a simple rendezvous server that is transparent to the user and operates without any user intervention. The server has the sole purpose of sitting on the network for the clients to register with and to distribute those registration details to all other clients. This allows the clients to discover the other clients it can connect with and their associated user details. The server only listens for one type of message, the “REGISTER” message, sent by the client applications. The server is intended for use in a hierarchical fashion, reflecting the natural hierarchy of the rescue team (as shown in Figure 1). In other words, separate instances of the server reside at the HQ, at the command posts (rescue vehicles) and on the devices of each search group leader. In this way, the voice service can still be used at level n of the hierarchy if connectivity to level n-1 is lost or not present.

Unfortunately, the server does not yet have any built-in security even though it would be globally reachable. This does leave it vulnerable to attack and would require additional security modules to be used in a production network.

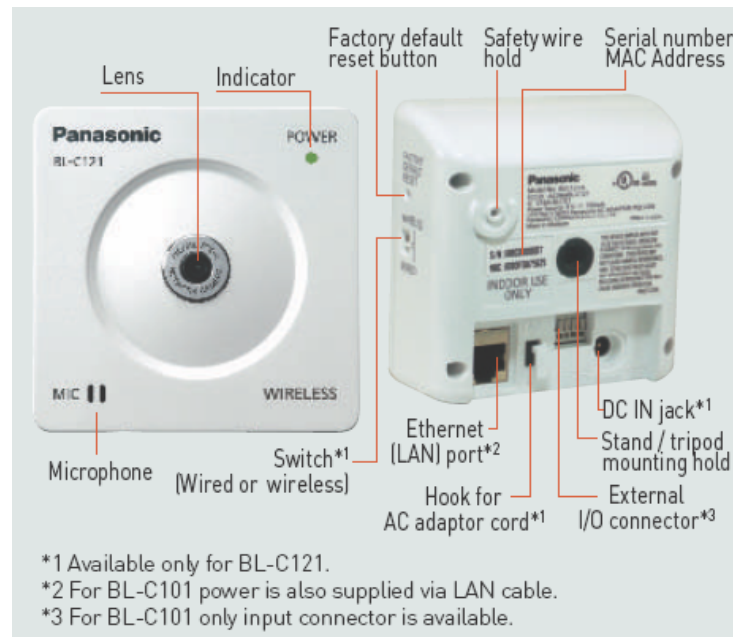
For further information on the implementation of the voice service, please refer to D4.2.1 Report on the Mountain Rescue Service Concept [8].

## 4.8. Video and Picture Services

Throughout various consultations with members of the CMRT, the concept of implementing real-time video and picture services gained increasing popularity. Whilst video and picture services were not deemed a critical requirement in the Mountain Rescue scenario, the ability to transmit live video footage and images of mountain conditions or the location/condition of a casualty was seen as highly desirable.

The main issues for the mountain rescue scenario are 1) finding a suitable video camera and 2) managing the resources within the network with respect to the data rates used by the video source. The video camera needs to be lightweight, waterproof, wearable, wireless, IPv6-compliant and capable of transmitting compressed video (rather than raw video) at various levels of quality. When the video source roams around within the MANEMO network, various levels of network capacity will be available at various points in time. The ability to adapt to this (e.g. by tuning up/down the transmitted video quality) is essential.

We chose the Panasonic BL-C101 and BL-C121 network cameras to use for the video service, as not only do they satisfy most of the requirements but also they are relatively inexpensive and easy to work with. Furthermore, they are also capable of providing the picture service. The two camera versions are almost identical with the main difference being that BL-C121 (Figure 28) is wireless.

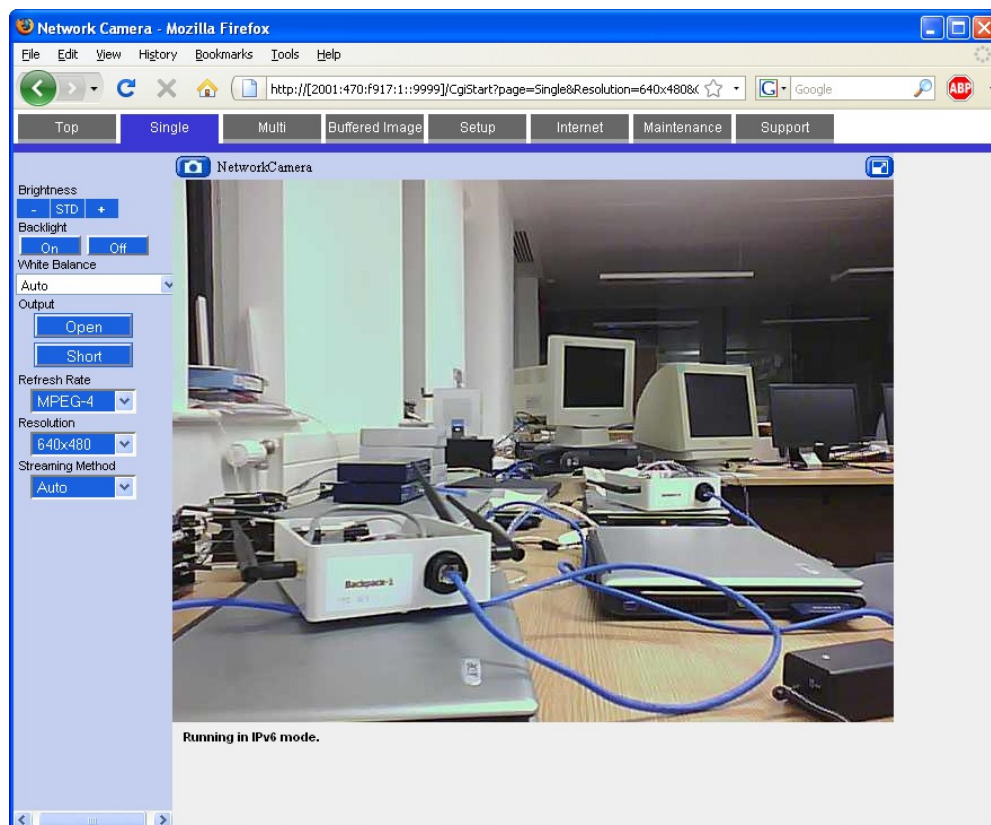


**Figure 28 Panasonic BL-C121 Network Camera [16]**

The Panasonic BL-C101 and BL-C121 features can be summarised as:

- The small, lightweight design allows the camera to be placed unobtrusively in any location and can be easily adapted into a wearable device.
- The 2-pin input connector can be used to connect the camera to an external trigger such as a sensor or manual switch to initiate the image or video transfer. This is particularly useful for situations when the video is ‘pushed’ to the CaC software due to some event rather than relying on a mission coordinator needing to request the data.
  - An Alarm Notification Sound can also be triggered at the receiver thus bringing the data to the attention of the mission coordinator.
- MPEG-4 support: Both cameras support MPEG-4 video compression enabling them to deliver fast moving live video at up to 30fps at full resolution. They are also dual-streaming so both a MJPEG and a MPEG-4 stream can run concurrently using independent image settings.
- Full Screen mode: Each camera has a full-screen mode, which enlarges the live image to the size of the recipients screen, allowing for more efficient monitoring.
- 1-way Audio: Both cameras support 1-way audio using a built-in microphone. This allows the audio from any location to be transmitted along with the video.
- SSL Support: The camera can send its images and data using SSL encryption across the network for greater security. Encrypting the data makes it much more difficult for someone to intercept and view the data while it is travelling around the network.
- IPv6 Support: To future-proof the camera it supports the latest protocol IPv6 as well as support for IPv4. Probably not required right now, but will be handy to have as we migrate to IPv6 addresses in the future.
- Image resolution and quality settings can be adjusted to requirements, which is important for adapting to changes in network capacity.

- Colour Night View Mode for increased brightness in low-light conditions. This is particularly useful for the Mountain Rescue scenario as many searches are conducted in low-light conditions.
- Image compression: JPEG (Motion JPEG), MPEG-4.
- Supported resolutions: 640x480 (VGA), 320x240 (default), 192x144.
- Frame rate: Max. 30fps (640x480 in MPEG-4 only, 320x240, 192x144).
- Audio compression: ADPCM 32kbps
- Wireless connectivity: IEEE802.11b/g, 13channels, up to 54Mbps (BL-C121).
  - Wireless security: SSID, WEP (64/128/152bit), WPA-PSK (TKIP), WPA2-PSK (AES).
- Security: multi-level user authentication with username/password entry, SSL.
- Protocols supported IPv4: TCP, UDP, IP, HTTP, FTP, SMTP, DHCP, DNS, ARP, ICMP, POP3, NTP, UPnP, SMTP Authentication, RTP, RTSP, RTCP, HTTPS, SSL, TLS. IPv6: TCP, UDP, IP, HTTP, FTP, SMTP, DNS, ICMPv6, POP3, NDP, NTP, RTP, RTSP, RTCP, HTTPS, SSL, TLS.
- Image transfer method: SMTP, FTP, HTTP.
- Alarm triggers: Alarm, timer or motion detection.
- Dimensions: (HxWxD) 85 x 85 x 27mm. Weight (unit only): 100g (0.22lb).



**Figure 29 Screenshot of the Video Web Service (Panasonic BL-C121)**



The wired version of the camera (BL-C101) can plug directly into the LAN port of the backpack router worn by a rescue worker. For this reason, the UTP cable connecting the camera to the router must be sewn into the backpack material to prevent any accidental snagging by the rescue worker. Alternatively, the wireless version of the camera (BL-C121) removes the need for any cabling as the camera simply connects to the PAN-assigned Wi-Fi interface of the backpack router and becomes part of the rescue worker's PAN. Using the wireless camera also has the advantage that a rescue worker with a camera is not required to wear a backpack router, provided he/she is within range of one. Similarly, a camera can be detached from the rescue worker and placed in strategic locations provided it has suitable wireless access somewhere within the IAN.

Rather than having to connect the camera to the backpack router and place extra drain on the latter's battery, we use a separate 9v PP3-size battery to power the camera. It is a simple matter to connect the PP3 pad to a 2.5mm jack plug for the camera's DC power socket.

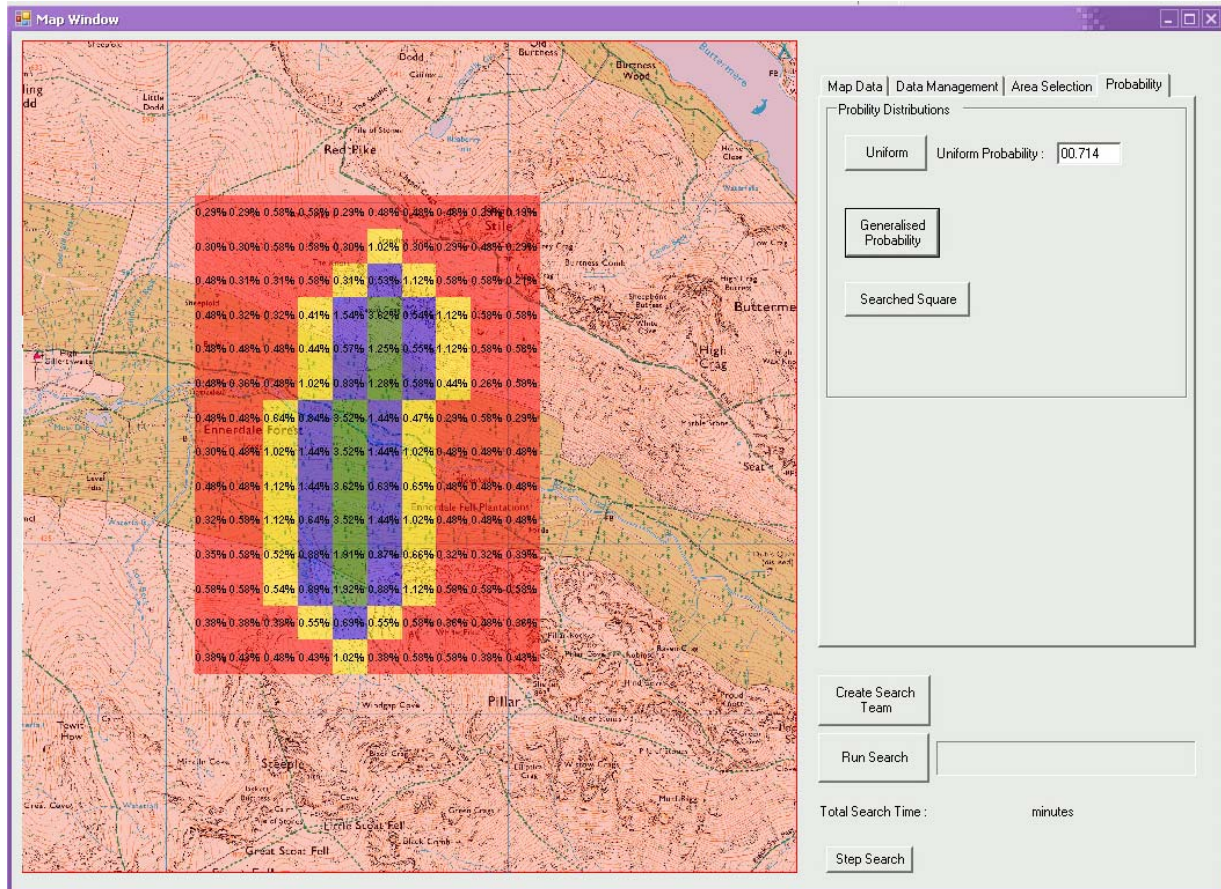
Ideally, the camera should be mounted onto a helmet that the rescuers wear. We have not yet determined a suitable way of doing this so that the camera is secured firmly. For the time being, we attach the camera to the central strap of a backpack so that the camera is looking forward from the rescuer's chest level. This also allows the rescuer to easily adjust or re-fasten the camera should it come loose.

## 4.9. Search Theory

There is considerable existing work on applying search theory techniques to a search and rescue (SAR) domain such as Mountain Rescue. However, this is mostly theoretical and usually based on 2-dimensional search areas (e.g. forests, deserts). In u-2010 we have investigated and developed appropriate search heuristics and algorithms applicable to 3-dimensional terrain (i.e. altitude is a factor). Combined with statistical techniques (applied to a previous incidents knowledge database), this would suggest realistic and practical search patterns for groups of rescue workers for a given incident. The number of rescuers and their relevant skills/experience is an additional input to the software.

The search theory software component takes into account previous incidents and makes use of both previous statistical data about the area in question, and specially designed heuristics, taking into account the terrain, status of the lost subject, weather interference, and other similar factors. This use of probability can be extrapolated and expanded to very complex levels, and prove invaluable in the algorithms used in the software, as search-and-rescue is heavily based on both initial information (the area to be searched, the last known position of the lost person), as well as additional observed information. For instance, the probability of a lost individual being in a certain area will decrease a great deal once that area has been searched once without success. Other factors, too, such as the finding of discarded personal items, have a great part to play in the probability adjustments, increasing the probability of finding the subject in areas near to where the evidence is found.

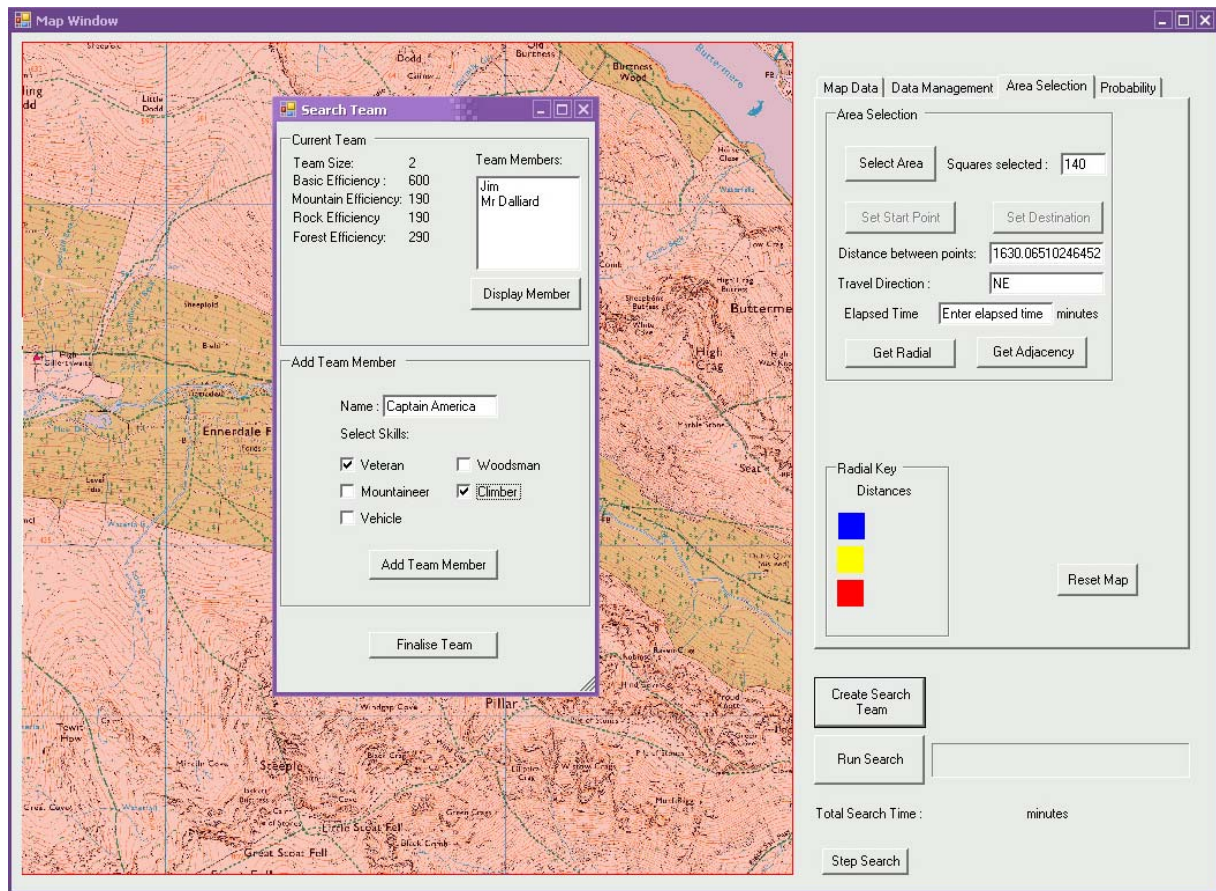
The probability of successfully finding the subject can be modified by numerous factors, such as (in maritime searches) the depth and clarity of the water, the roughness of the sea, etc., and in land-based search and rescue, factors such as the amount of ground foliage, the weather, the ease of actually getting to the area to search, etc.



**Figure 30 Probability distribution**

The search theory software component works in harmony with the PMS and Alarm service. Once the information gathered from an emergency call is entered into the Alarm service, the search theory software parses this information and checks it against information already held in the database. Combined with the responses observed by the Alarm component, the search theory software suggests optimum search patterns and locations with respect to the number of rescue workers responding to the call.

Ultimately, the search theory software allows probability maps to be generated according to different methods (e.g. Figure 30), the development of search routes for these maps, and the creation of search teams generated from responses to the Alarm system (Figure 31). Thus, we are able to plan a search of an area to be as efficient as possible and yield the highest chance of finding the lost subject as rapidly as is feasible.



**Figure 31 Assigning a Search Team**

Certain priorities and general operational strategies are used by rescue teams when seeking a lost subject, and a number of these are implemented in the system. For instance, when a subject's last position and intended destination are known, one of the first steps will be to search along this path and areas near it, as well as any accident black spots along the route (accident black spots are gathered from the previous incidents knowledge database).

Of course, the Mountain Rescue team may wish to disregard suggestions from the search theory software and instead manually determine the most effective method of searching an area rapidly. This is enabled by providing a user-adjustable confidence setting within the application.


## 4.10. What Will Not Be Implemented

Due to timing and resource constraints, the following services will not be implemented in time to be included in the Mountain Rescue Service trial.

### 4.10.1. Sensor Service

There is scope to have biomedical sensors incorporated into the Mountain Rescue scenario. For example, sensors attached to the rescue workers can relay information pertaining to their condition (e.g. heart rate, body temperature) to the mission coordinator. Similarly, once a casualty is located, biomedical sensors



	<p align="center"><b>D4.2.2 Prototype Mountain Rescue Service Trial</b></p>	
---	---	---

could relay all available medical data to waiting paramedics, ambulances or the emergency room at the hospital.

Although we have managed to integrate sensor network capability into the backpack routers (see section 4.2), we do not have enough resources to fully integrate this into a demonstration with suitable body sensors attached to rescue workers and casualties.

#### **4.10.2. Directory Service**

We have the intention to integrate all the other services (e.g. presence management, voice services, network services, search theory) with Directory Services. This would essentially replace the need for services to directly access the SQL database that we currently use. However, it is uncertain whether this would be achievable within the remaining lifetime of the project.

#### **4.10.3. Integrated Voice Service**

Although we have implemented a rudimentary voice service for the Mountain Rescue scenario, this has not been integrated with the CaC software backend and the PMS. Ideally, the mission coordinator should be able to establish one-to-one and group calls by selecting the appropriate members displayed on the CaC GUI. Moreover, the implemented voice service does not yet interoperate with the PSTN or cellular phone networks.

## 5. Trial Methodology

The purpose of the Mountain Rescue service trial is to verify the operational working of the prototype implementation and to validate that the technical and user requirements, specified in D1.1.2 Functional requirements for networks and services [2], have been met.

The Mountain Rescue service trial is conducted in two ‘flavours’. The technological aspects of hardware, software and network protocols are tested by technical staff in both laboratory and field environments. Meanwhile the operational aspects are tested in the field, first by technical staff and second by end users, that is, members of the CMRT.

The high-level objectives of the trial can be summarised as:

- Establish and maintain successful network connections from the mountains to HQ
- Network connections can be deployed rapidly
- No network or device configuration required by users
- Reasonable mission lifetime across the system
- Connectivity maintained when roaming in mountains
- Sufficient voice service across network
- Sufficient video and image service across network
- Successful presence management / localisation service across network
- Suitable command and control backend solution

We therefore conduct technical oriented tests of all the individual prototype systems before conducting technical and user oriented tests of the integrated systems.

### 5.1. Presence Management Service Tests

The main objective of testing the Presence Management Service is to verify that location updates can be sent from user devices in the mountains to the software hosted at the Team HQ. Further objectives include the ability for the client software to use the best available communications medium and for the system to recover when periods of no connectivity are seen.

The testing of the PMS consisted of three phases comprising initial lab tests, preliminary field tests and on-mountain tests with the IAN connected to the Team HQ.

Entering the field testing phase after elementary lab tests, we tested the system in the region that the CMRT operates in by emulating search patterns of rescue missions. In all of our field/mountain tests, we disabled the GPRS functionality on the PDA devices for two reasons: 1) to avoid the GPRS to Wi-Fi swapping bug in Windows Mobile and 2) because GSM signals in the region are generally not good enough to establish or maintain GPRS connections.

In a preliminary test before we had established our on-mountain IAN, we conducted a walk and drive around the areas of Buttermere, Scale Bridge, Scale Hill and Lorton (appropriate areas for CMRT operations). During this 125 minutes trial the client application used both online and offline mode.

A further on-mountain experiment was carried out using an on-mountain Wi-Fi network testbed for several hours in the area of Buttermere. During this experiment, a person was monitoring the server



	<p align="center"><b>D4.2.2 Prototype Mountain Rescue Service Trial</b></p>	
---	---	---

application running at the University tracking the movements of the users roaming in and out of the on-mountain network.

More recent tests have been conducted integrated with the deployment of the Incident Area Network, establishing uplink connections to CLEO and GEANT (via the Astra2Connect satellite service), with the server located at the Cockermouth HQ.

In the most recent tests, we have consolidated the test parameters from which the results will be analysed:

- PMS client module synchronisation with GPS satellites
  - average time taken from activation to give a location
  - differences between devices used
  - how stable are the GPS signals in mountains?
- Reported GPS locations verified for accuracy
  - checked against Garmin readings
  - checked against map readings
  - checked against Google maps (server end)
- Location updates sent using Wi-Fi when available
  - client monitors connection to server to verify it is reachable
  - client swaps to using SMS when Wi-Fi is unavailable or server is unreachable over Wi-Fi
- Client stores all locations and timestamps
  - client updates server after periods with no connectivity available
- Determine how many updates are lost
  - Wi-Fi vs. SMS reliability

## 5.2. Backpack Router Tests

The backpack routers perform a crucial role in the IAN of the Mountain Rescue service trial. It is therefore important to test that they meet their design objectives. These can be summarised as:

- Size. The router enclosure must be small enough to fit easily inside a backpack compartment.
- Weight. The router must be light enough to be carried by rescue workers on long search and rescue operations.
- Boot time. The time taken for the router to be usable after it has been switched on should be as fast as possible.
- Easy to use. The user should not have to perform any configuration nor need any significant training to operate the router.
- Battery lifetime. The router should be able to operate for several hours in order to be useful for search and rescue operations.
- Reliability. The router should not reset or hang.

	<p align="center"><b>D4.2.2 Prototype Mountain Rescue Service Trial</b></p>	
---	---	---

- Vibration and shock. Shocks and vibrations from walking, running and climbing should not affect the operation of the router.
- Weather resistance. The router should be resistant to weather conditions i.e. wind, rain, frost and sunshine.
- Effective range. The radio hardware inside the routers of backpack radio modules and antenna combinations

Suitable laboratory and field tests to verify these goals have been conducted throughout the summer of 2009. The results of these are reported in D4.2.3.

### 5.3. Satellite and Backhaul Link Tests

The satellite and backhaul links connect the Incident Area Network to the Team HQ, allowing communication from the mountains to the Team HQ. The main objectives of these links are:

- Satellite dish and receiver can be setup and configured rapidly.
  - time to setup dish, stand and receiver
  - satellite synchronisation time
  - time for first packet to be routed from arrival at location
- Size and weight of satellite equipment
  - storage requirements
  - problems with dish size (high winds)
- Location requirements
  - LoS to satellite
  - Estimated required distance from mountainside for LoS
- Data performance of satellite link
  - in different weather conditions
- Radio backhaul links can be setup and configured rapidly
  - time to setup antenna, stand and receiver
  - antenna pointing and link synchronisation time
  - time for first packet to be routed from arrival at location
- Size and weight of radio equipment
  - storage requirements
  - can the remote relay be easily carried?

For the satellite link, we have conducted numerous tests both at Lancaster University and in the Buttermere area of the CMRT search region. Tests have consisted of timed link establishment from the point when the equipment is removed from a vehicle to the point when the first packet is routed over the link. These tests have also been conducted in various weather conditions, with high winds proving to be

	<p align="center"><b>D4.2.2 Prototype Mountain Rescue Service Trial</b></p>	
---	---	---

the most challenging. Moreover, the data performance of the satellite link in different weather conditions has been tested for both IPv4 and IPv6-in-IPv4 traffic.

The radio backhaul links have been tested to verify that they can be used as ‘rapid response’ PoPs. Since the hardware and assembly have to be carried to the relay location, numerous tests have involved carrying a backpack of equipment to pre-determined locations on the mountainside and establishing the radio link for the IAN uplink to the WAN. Since portable generators are too heavy to carry a reasonable distance, the batteries have been tested to determine the expected uptime of the radio link for various levels of link utilisation.

## 5.4. Command and Control Software Tests


The command and control (CaC) software is located at the Team HQ and provides a central point for various services including the Alarm Service, the PMS, Video Service and GIS. The objective of these tests is to verify that these services are operating satisfactorily:

- AlarmTILT Integration
  - Emergency operations can be launched and terminated using AlarmTILT
  - Available members are contacted using AlarmTILT
  - Software monitors responses from members and notifies them upon closure.
- GIS
  - Mapping engine displays all OS details
  - Maps have zoom in/out, scroll and rescale capability
- Presence Management Service
  - Mapping and navigation using GIS is accurate
  - All rescue worker movements are logged
  - Missions can be replayed from logs
- Instant messaging
  - Messages can be sent and received using IPv6 and SMS
- Video and Picture service
  - Web service showing video streams and pictures from remote cameras controlled from CaC software

## 5.5. Voice Service Tests

The objectives of the VoIP voice service tests are as follows:

- Identify how well the VoIP service performs using numerous wireless hops and different backhaul connectivity options.
- Identify the effect of signal degradation, channel interference and link utilisation on the VoIP service performance.

	<p align="center"><b>D4.2.2 Prototype Mountain Rescue Service Trial</b></p>	
---	---	---

- Determine if it is possible to run a VoIP service in a MANEMO infrastructure and how feasible this is.
- Compare the bespoke voice service with a CoTS solution (Linphone).
- Identify situations where QoS may be suitable or even necessary in order to achieve an acceptable VoIP service.
- Determine whether push-to-talk emulation provides a more robust voice service than an open access, full duplex system. What is the optimal trade-off between user familiarity, system robustness and feature richness?

### 5.5.1. Test Procedures

All voice service tests are carried out using pre-recorded audio files in addition to unscripted user conversations. Using pre-recorded audio files allows a more exact measurement and analysis of data such as packet latency and loss, since the content and semantics of the data is known in advance. Repeating the tests with unscripted user conversations allows us to gain a more qualitative insight into the voice service performance based on user experience.

In order to make a comparison with a CoTS VoIP solution, we needed to find a non-commercial IPv6-capable VoIP application. This application has to be IPv6 capable in order to operate over MANEMO as required. Ideally, this application would run in the Windows Mobile environment so the same client devices could be used which would eliminate any hardware or OS performance differences. Unfortunately, no suitable application could be found that matched the criteria exactly. Ultimately, Linphone was chosen as the comparison application as it had all the desired functionality but only varied in the device and OS that it operates on.

This means all tests are performed with PDAs running Windows Mobile and the custom VoIP service and with Linux laptops using the Linphone application.

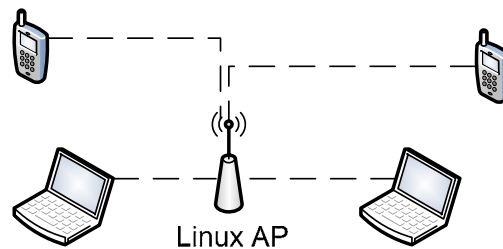
All tests are performed with mobility in mind. The devices are only connected via a wireless access point and varying scenarios of backend connectivity. They move in a pattern designed to push them in and out of connectivity to see what happens in each situation. At first, the devices start close to the access point and then are taken close to the edge of signal range. They are then taken out of range before being slowly brought back into range again. The final point is to attempt to place the device right on the cusp of the wireless signal to observe the effect on the VoIP service.

RTT measurements for different test scenarios are taken using a ping utility. Packet data at the endpoints is recorded using the Wireshark network measurement tool in order to compare data rates and packet losses. Ideally, this would be on the clients themselves but this is not possible with the Windows Mobile PDAs. Therefore, data is captured at the first and last router the data passes through in order to compare loss on the backhaul. Sequence numbers for voice data will be used to determine packet loss in the test scenarios. The tests are performed with as little network traffic as can be achieved in order not to affect the results. The only exception to this is when background traffic is injected into the network to see if the applications could benefit from QoS.

### 5.5.2. Test Scenarios

This initial testing stage consists of using a single Linux PC with a wireless network adaptor to broadcast an IPv6 enabled wireless network. The devices we have chosen to use, 2x Windows Mobile PDAs running the custom VoIP application and 2x Linux laptops running Linphone, are set up ready to connect to each other. On the Linux PC, Wireshark is used to log to all packets from the connected devices. Each

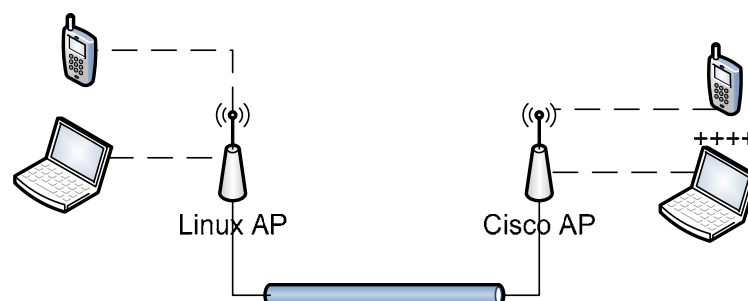
pair of devices are then connected in turn and used to run the tests while the data is recorded. The purpose of this stage is just to test both applications function correctly with no errors and to give a base for data rate comparison for later tests. The topology of the network set up being used for this stage can be seen in Figure 33.



**Figure 32 Voice Service - Local Initial Testing**

After the initial set of tests, the focus moves to a more complex sets of tests with gradually increasing phases of complexity. The next phase is to see how the applications handle a simple wireless network situation where there is an Ethernet connection as a backbone link. The setup consists of a Linux PC with a wireless network adaptor acting as an access point connected to a Ethernet backbone which has a connection to a Cisco wireless access point. The entire network is IPv6 enabled in order to support MANEMO that is used later. This setup can be seen diagrammatically in Figure 33.

In this stage a test using ping6 to determine RTTs between the devices is performed. This is followed by the basic audio tests which consist of the playout of the audio files and users conversing using the applications. These are close to the access points so the effect of the wireless determination is not a considerable factor. This allows results to be taken about how the VoIP is coping with the backhaul medium and its effect. Once these are completed, mobility tests take place. Firstly with one device from each pair moving as described and then with both devices moving in this fashion. This will show the effect of the wireless signal and quality on the voice applications compared to the results they had with strong signal and no loss in the previous test. When these have been completed, the same set of tests are performed again, this time running IPERF over the backhaul connectivity medium. In this case, UDP packets are generated in ever increasing frequency to simulate heavy traffic on the backhaul. This is done in increments until the VoIP degrades so much that it is unusable.

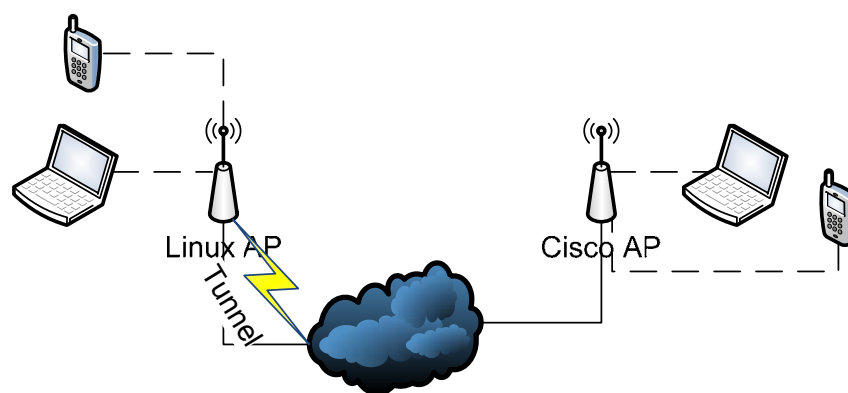


**Figure 33 Voice Service – Local Base Tests**

In the following stage we run the same set of tests but with a more complex backhaul medium. Instead of an Ethernet backhaul link, the global Internet is used. In order to give us a suitable number of hops an IPv6-in-IPv4 tunnel is used with a provider that is a certain topological distance from the UK. This is



done for two purposes. It introduces the random traffic element to the tests so they can be compared to previous tests where the traffic was controlled and increasing the number of network hops the traffic has to go through, increasing the traffic delay and the chance that the packets will be lost in transit. Firstly, a tunnel is established from Lancaster to London (or another nearby European city) in order to increase the hops and delay by only a short amount to emulate a standard VoIP call in the UK. After this, the tests are then repeated with a much longer tunnel (e.g. to Hong Kong) in order to get a long a delay as possible and a very high latency. This helps to emulate a long distance VoIP call. Finally, running the tests involving a satellite link, using the Astra2Connect service, gives us a valuable set of results for VoIP calls when a satellite backhaul is the only option (quite possible in a Mountain Rescue context). Again this set of tests is run without MANEMO present so we have a base comparison for these scenarios when the MANEMO tests are run using the same situations.



**Figure 34 Voice Service - Internet Tests**

Once this stage has been completed, we should have a solid baseline for comparison when we introduce MANEMO. These tests are part of the systems integration tests and so are described in section 5.8.

## 5.6. Video Services Tests

The test of the Video Service can be summarised as:

- Verify video server can transmit video over IPv6
- Verify that the observed images and video are of sufficient quality
- Observed data rates when using
  - Different encoding schemes
  - Different video resolution
- Streaming method
- Stability of the camera when attached to backpack
- Average battery uptime when streaming continuously
  - Wired vs. wireless camera
  - Video resolution vs. power consumption
  - Encoding method vs. power consumption

- Streaming method vs. power consumption

## 5.7. MANEMO Tests

The MANEMO protocol suite we have implemented is the core technology behind the role of the backpack routers. The successful operation of MANEMO is therefore critical to the success of the Mountain Rescue service trial. In summary, the tests of the MANEMO software are:

- Ensure the MANEMO protocols operate without crashing or hanging the router
- Verify that MANEMO can operate with user configuration or intervention
- Verify that MANEMO is able to connect to networks that have not been pre-configured
- Verify that MANEMO can provide routing between the Mobile Command Post and the WAN via the IAN
- Handover management
  - Certify the handover manager can monitor all available connectivity options
  - Ensure the handover manager monitors L3 connectivity to its Home Agent
  - Ensure the handover manager does not connect to incorrect, undesirable or sub-optimal networks
  - Examine how optimal the behaviour of the handover manager is
  - Conduct handover latency tests to determine impact on voice and video services
- Examine the effect of mobile chaining
  - What are the realistic possibilities for extending the IAN from the Mobile Command Post?
  - How far away from the Mobile Command Post given n Mobile Units?
- Identify any scenarios (however unlikely) that MANEMO cannot solve or where MANEMO is no the optimal solution.

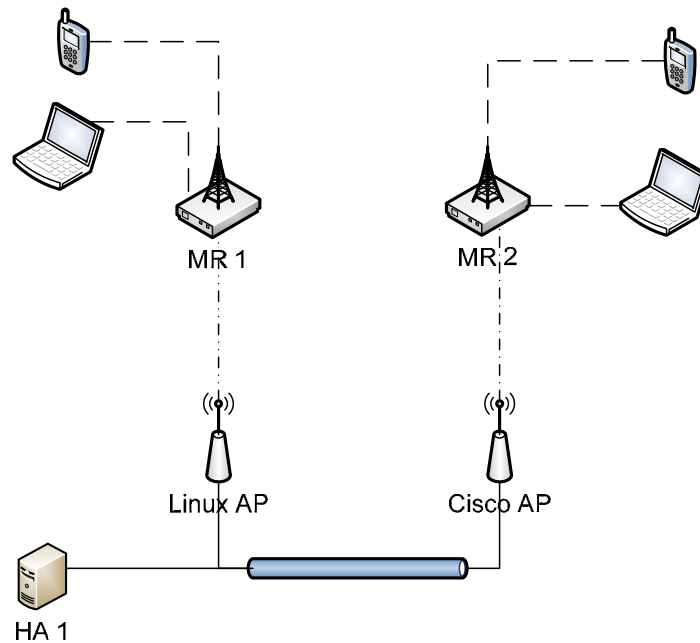
## 5.8. MANEMO and Voice Service

Further to the elementary Voice Service tests, further tests over a MANEMO infrastructure are required to try to determine if a VoIP-like service is feasible in a MANEMO environment.

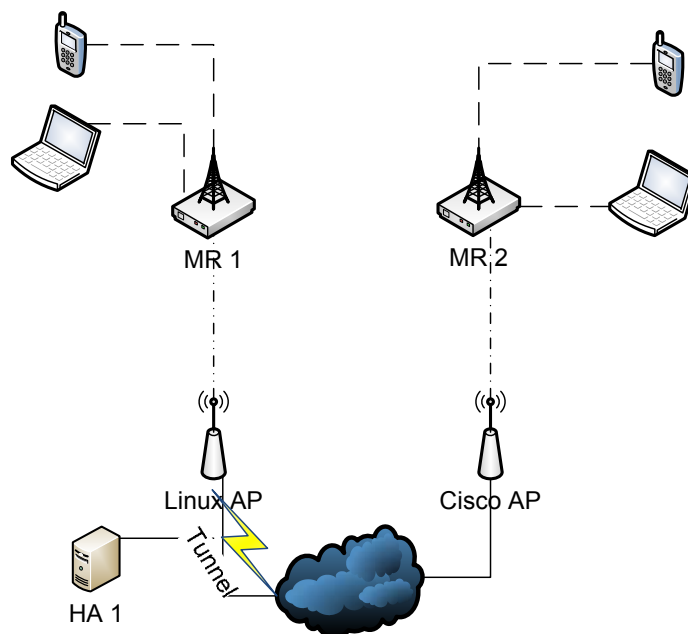
This consists of two separate backpack routers (representing separate mobile networks), with the user devices connected to these routers. In addition, a Home Agent is located on the network, which provides a mobility service for both backpack routers. The setup of this can be seen in Figure 35.

In this setup the same standard set of tests is run as described for previous Voice Service tests. The initial set of tests is compared to the tests from previous stages to see what effect the MANEMO protocol set has on the VoIP traffic and if any issues have arisen over the wireless connection. The extra tests are concerned with movement of the backpack router to which the devices are connected. For the first set of tests, the user devices will stay close to their backpack routers so wireless packet loss is limited and the backpack routers (not the user devices) will be moved in the mobility pattern described earlier. This allows us to see how MANEMO itself affects the voice connections, as the actual user devices (PDA's and Laptops), will maintain the same wireless connection to their associated backpack router. The final

test for this stage is to get MANEMO to perform a network handover of a backpack router. This involves one backpack router moving out of range of the Linux AP and connecting to the Cisco AP.



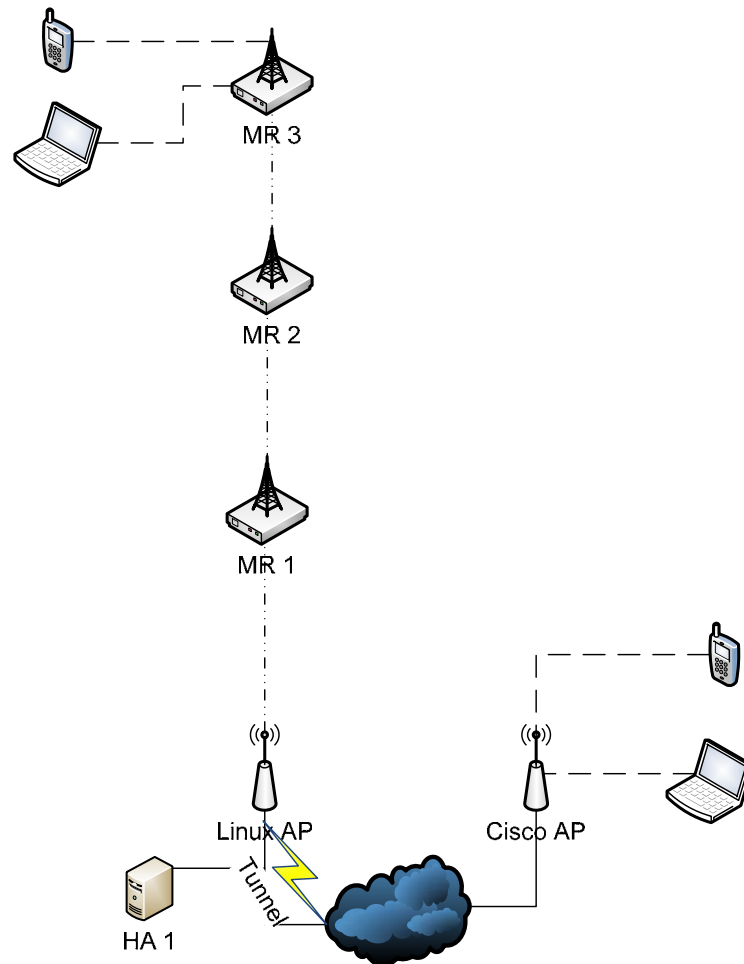
**Figure 35 Voice Service and MANEMO**



**Figure 36 Voice Service and MANEMO – Long distance**

Additional complexity is introduced by adding a large delay link to emulate a VoIP call over a large distance. This is accomplished by adding a satellite link (and the necessary IPv6-in-IPv4 tunnel) at the egress of one access point (Figure 36). As before, this is to introduce a large number of hops in the

backhaul connectivity medium. One backpack router is able to access the Home Agent locally, while the other has to traverse the tunnel to reach it.





**Figure 37 Voice Service - Large Number of Wireless Hops**

A final set of tests uses the same backhaul setup as in the previous tests but with a chain of mobile routers attached to one of the access points (Figure 37). This is to emulate the situation where the IAN is extended into a search region by the movement of the rescue workers carrying backpack routers. Thus, there will be multiple wireless hops that are introduced to the IAN for some end-to-end paths. Tests initially use a chain of three backpack routers, with a view to determining how long the chain can be before VoIP performance becomes intolerable.

Finally, a handover of the entire mobile router chain takes place to see what effect this has on the VoIP service. The effects of a handover with such a large amount of wireless hops should provide interesting results.

## 5.9. MANEMO and Video Service

Similar to testing MANEMO with the Voice Service, the performance of the Video Service in a MANEMO environment is also to be investigated. Although the latency requirements of the video streams

	<p align="center"><b>D4.2.2 Prototype Mountain Rescue Service Trial</b></p>	
---	---	---

are not as critical as with VoIP, there is still an open issue to investigate regarding the behaviour of the video streams in the presence of multiple wireless hops and long distance links (e.g. satellite).

Perhaps, more interesting from an evaluation perspective is the effect on video stream performance due to changes in available data rates. The unpredictable nature of multiple wireless hops in the IAN, long distance links across the WAN and handover events, all contribute to large variations in available data rates over time. This can lead to packet loss and high latency/jitter especially when streaming over TCP.

For these reasons, we use the same test infrastructures as the Voice Service tests in the previous section to test the Video Service performance. However, the Video Service tests will concentrate on effect on different stream resolutions and encodings in the presence of multiple wireless hops, long distance links and handover events. Each of these tests is repeated for the different streaming options available (UDP, HTTP etc.).



## References

- [1] U-2010 Deliverable 1.1.1, “Reference scenarios based on user studies”, October 2007.
- [2] U-2010 Deliverable 1.1.2, “Functional requirements for networks and services”, March 2007.
- [3] U-2010 Deliverable 2.1.2, “u-2010 Architecture”, June 2009.
- [4] U-2010 Deliverable 2.2.2, “Report on u-2010 Mobility Solution”, February 2009.
- [5] U-2010 Deliverable 3.2.1, “Report on the Presence Management Solution”, November 2008.
- [6] U-2010 Deliverable 3.2.2, “Prototype of the Presence Management Solution”, November 2008.
- [7] U-2010 Deliverable 4.1.1, “Prototype of an alarm and emergency communication system based on the developed architecture and services in Luxembourg”, November 2008.
- [8] U-2010 Deliverable 4.2.1, “Report on the Mountain Rescue Service Concept”, July 2008.
- [9] U-2010 Deliverable 4.2.3, “Report on the Mountain Rescue Service Trial”, September 2009.
- [10] U-2010 Deliverable 4.5.2, “Report on Mountain Rescue Service Implemented in Slovenia”, September 2009.
- [11] Cockermouth Mountain Rescue FAQ, Available From:  
<http://www.cockermouthmrt.org.uk/faq.aspx#faq4>
- [12] <http://www.speedtest.net/>
- [13] <http://www.broadbandspeedchecker.co.uk/>
- [14] <http://www.thinkbroadband.com/speedtest.html>
- [15] Hurricane Electric Internet Services IPv6 Tunnel Broker, <http://ipv6tb.he.net/>
- [16] Panasonic BL-C101, BL-C121 Product Brochure.
- [17] Ubiquiti Routerstation homepage <http://www.ubnt.com/products/rs.php>
- [18] Ubiquiti Routerstation Pro homepage <http://www.ubnt.com/products/rspro.php>
- [19] “Grayrigg Train Crash”, [http://news.bbc.co.uk/2/hi/uk\\_news/6391633.stm](http://news.bbc.co.uk/2/hi/uk_news/6391633.stm)

## Acronyms

2D	2-Dimensional
3D	3-Dimensional
3G	3 <sup>rd</sup> Generation (of mobile phone technology and standards)
ANSI	American National Standards Institute
AP	Access Point
API	Application Programming Interface
AR	Access Router
CANLMAN	Cumbria And North Lancashire Metropolitan Area Network
GIS	Geographical Information System
CLEO	Cumbria and Lancashire Education Online
CMRT	Cockermouth Mountain Rescue Team
CoTS	Commercial off-the-Shelf
CODEC	Coder Decoder
DC	Direct Current
EDGE	Enhanced Data Rate for Global Evolution
ESSID	Extended Service Set Identifier
EU	European Union
GCC	GNU Compiler Collection
GPRS	General Packet Radio System
GPS	Global Positioning System
GSM	Groupe Spécial Mobile (Global System for Mobile Communications)
GUI	Graphical User Interface
HA	Home Agent
HCI	Human Computer Interface
HD	High Definition
HQ	Headquarters
HSDPA	High Speed Downlink Packet Access
HTTP	Hypertext Transfer Protocol
IAN	Incident Area Network
ICT	Information Communication Technology
ID	Identifier
IETF	Internet Engineering Task Force

IOS	Internetwork Operating System
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
JPEG	Joint Photographic Experts Group
LoS	Line of Sight
MAC	Medium Access Control
MANEMO	MANET for NEMO (alternative: MANET and NEMO)
MANET	Mobile Ad-hoc Network
MCM	MANET-Centric MANEMO
MIPv6	Mobile IPv6
MP3	MPEG-1 Audio Layer 3
MPEG	Motion Picture Experts Group
MJPEG	Motion JPEG
MR	Mobile Router
NCM	NEMO-Centric MANEMO
NEMO	Network Mobility
NEMO BS	Network Mobility Basic Support
NEPL	NEMO Platform for Linux
NINA	Network in Node Advertisement
OS	Operating System
OS	Ordnance Survey
PAN	Personal Area Network
PC	Personal Computer
PDA	Personal Digital Assistant
PMS	Presence Management Service
PoE	Power over Ethernet
PoP	Point of Presence
PMS	Presence Management System
PSTN	Public Switched Telephone Network
RF	Radio Frequency
RO	Route Optimisation
RSSI	Received Signal Strength Indicator
RTT	Round Trip Time
SAR	Search and Rescue

SBC	Single Board Computer
SDIO	Secure Digital Input Output
SDK	Software Development Kit
SIP	Session Initiation Protocol
SMRA	Slovenian Mountain Rescue Association
SMS	Short Message Service
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
SSL	Secure Sockets Layer
SSID	Service Set Identifier
STA	Search Theory Automatisation
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UK	United Kingdom
UMF	Unified Message Format
UMA	Unified MANEMO Architecture
UMTS	Universal Mobile Telecommunications System
UTP	Unshielded Twisted Pair
USB	Universal Serial Bus
VAR	Voice Activity Detection
VBR	Variable Bit Rate
VoIP	Voice over IP
WAN	Wide Area Network
WiFi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WPA	WiFi Protected Access
WPA-PSK	WPA Pre-Shared Key
XML	Extensible Markup Language